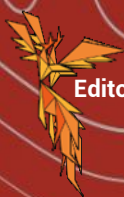
Direitos Fundamentais na Era Digital

Anuário 2023 das Comissões Especiais de Proteção de Dados (CEPD) e de Direito Digital (CEDD) da OAB

Laura Schertel Mendes
Fabrício da Mota Alves
Tainá Aguiar Junquilho
Rodrigo Badaró
Ingo Wolfgang Sarlet
Mônica Tiemy Fujimoto
Orgs.

Editora Fundação Fênix

A escolha do tema "Direitos Fundamentais na Era Digital" é uma forma de prestar uma homenagem e um tributo ao saudoso Professor e Advogado Danilo César Maganhoto Doneda, cuja contribuição inestimável para o debate sobre a efetividade dos princípios constitucionais na era digital é indiscutível. Sua obra de 2006, "Da Privacidade à Proteção de Dados Pessoais", foi pioneira no debate sobre proteção de dados no Brasil, reconhecendo há muito tempo a importância da tutela constitucional relacionada à proteção de dados pessoais. Por meio de sua pesquisa de excelência, perspectiva humanista e compromisso com a garantia dos direitos humanos, Danilo inspirou fortemente a construção do marco regulatório no Brasil, tornando-se uma figura central nas principais discussões sobre cidadania digital no país. Ele foi membro indicado pela Câmara dos Deputados para o Conselho Nacional de Proteção de Dados e Privacidade, participou das discussões sobre a elaboração do Marco Civil da Internet, foi coautor do anteprojeto da LGPD, integrou a Comissão de Juristas responsável pelo anteprojeto da LGPD Penal e a Comissão de Juristas (CJSUBIA) responsável por subsidiar a elaboração da minuta do substitutivo sobre inteligência artificial no Brasil. Sua relevância ultrapassou as fronteiras do Brasil, sendo o primeiro brasileiro a ser nomeado diretor da *International Association of Privacy Professionals* (IAPP), participando de importantes fóruns de discussão em todo o mundo e publicando artigos relevantes em grandes veículos acadêmicos.

Os Organizadores.

Editora Fundação Fênix

DIREITOS FUNDAMENTAIS NA ERA DIGITAL

Anuário 2023 das Comissões Especiais de Proteção de Dados (CEPD) e de Direito Digital (CEDD)

Organização

Comissão Especial de Direito Digital

Laura Schertel Mendes

Fabrício da Mota Alves

Tainá Aguiar Junquilho

Comissão Especial de Proteção de Dados

Rodrigo Badaró

Ingo Wolfgang Sarlet

Mônica Tiemy Fujimoto

DIREITOS FUNDAMENTAIS NA ERA DIGITAL

Anuário 2023 das Comissões Especiais de Proteção de Dados (CEPD) e de Direito Digital (CEDD)

Editora Fundação Fênix

Porto Alegre, 2023

Direção editorial: Ingo Wolfgang Sarlet
Diagramação: Editora Fundação Fênix
Concepção da Capa: Editora Fundação Fênix

O padrão ortográfico, o sistema de citações, as referências bibliográficas, o conteúdo e a revisão de cada capítulo são de inteira responsabilidade de seu respectivo autor.

Série Direito – 87

Catalogação na Fonte

D598 Direitos fundamentais na era digital [recurso eletrônico] : Anuário 2023 das Comissões Especiais de Proteção de Dados (CEPD) e de Direito Digital (CEDD) / Laura Schertel Mendes ... [et al.] Organizadores. – Porto Alegre : Editora Fundação Fênix, 2023.
284 p. (Série Direito ; 87)

Demais organizadores: Fabrício da Mota Alves, Tainá Aguiar Junquilho, Rodrigo Badaró, Ingo Wolfgang Sarlet, Mônica Tiemy Fujimoto.
Disponível em: <http://www.fundarfenix.com.br>
ISBN 978-65-5460-079-8
DOI https://doi.org/10.36592/9786554600798

1. Direito. 2. Inteligência artificial. 3. Proteção de dados. 4. Direito digital. 5. Direito fundamental. I. Mendes, Laura Schertel (org.).

CDD: 340

Responsável pela catalogação: Lidiane Corrêa Souza Morschel CRB10/1721

AUTORES

Alisson A. Possa
Cacyone Gomes Barbosa Gonçalves Lavareda
Debora Sirotheau Siqueira Rodrigues
Francisco Soares Campelo Filho
Gabrielle Bezerra Sales Sarlet
Ingo Wolfgang Sarlet
Jorge Alexandre Fagundes
Lécio Silva Machado
Leide Jane Macedo da Silva
Lucia Maria Teixeira Ferreira
Martha Leal
Melissa Barrioni e Oliveira
Stella Muniz Campos Elias

HOMENAGEADO

Danilo Cesar Maganhoto Doneda
Bacharel em Direito pela Universidade Federal do Paraná (1995), Mestre (1999) e Doutor em Direito pela Universidade do Estado do Rio de Janeiro (2004). Professor no IDP. Professor visitante na Faculdade de Direito da Universidade do Estado do Rio de Janeiro. Foi Coordenador-Geral de Estudos e Monitoramento de Mercado na Secretaria Nacional do Consumidor do Ministério da Justiça. Foi pesquisador visitante na Università degli Studi di Camerino e na Autorità Garante per la Protezione dei Dati Personali, ambas na Itália. Advogado. Co-autor do anteprojeto de lei que deu origem à Lei Geral de Proteção de Dados. Membro indicado pela Câmara dos Deputados ara o Conselho Nacional de Proteção de Dados e Privacidade. Membro da Comissão de Juristas formada pela Câmara dos Deputados para redigir projeto de lei sobre proteção de dados nos setores de segurança pública e investigação criminal. Membro da Comissão de Juristas responsável por subsidiar elaboração de

substitutivo sobre inteligência artificial no Brasil. Membro do Grupo de Trabalho sobre proteção de dados e informações judiciais do Conselho Nacional de Justiça. Membro dos conselhos consultivos do Projeto Global Pulse (ONU), do Projeto Criança e Consumo (Instituto Alana) e da Open Knowledge Brasil. Consultor do Comitê Gestor da Internet no Brasil (CGI.br). É membro do conselho editorial da Revista de Derecho Digital (Espanha).

COMITÊ CIENTÍFICO

Laura Schertel Mendes

É professora do Instituto Brasileiro de Desenvolvimento, Ensino e Pesquisa (IDP) e de direito da Universidade de Brasília (UnB) com doutorado na Humboldt-Universität zu Berlin. É Pesquisadora Visitante da Goethe-Universität Frankfurt am Main, Foi relatora da Comissão de Juristas responsável por assessorar o Senado Federal sobre a regulação da inteligência artificial no Brasil. É diretora do Centro de Internet, Direito e Sociedade do IDP, membro do Conselho Nacional de Proteção de Dados e Privacidade da ANPD (CNPD) e co-diretora da Associação Luso-Alemã de juristas (DLJV-Berlim). É presidente da comissão de direito digital da OAB Nacional.

Rodrigo Badaró

Advogado, com MBA pela FGV em Direito Empresarial. É um dos atuais representantes do Conselho Federal da Ordem dos Advogados do Brasil (OAB) no Conselho Nacional do Ministério Público (CNMP). No Conselho Nacional de Justiça (CNJ), integra a Comissão de Proteção de Dados. Integra o Conselho Nacional de Proteção de Dados (CNPD) na condição de representante da sociedade civil. Na OAB, é o atual presidente da Comissão Nacional de Proteção de Dados. Foi Conselheiro Federal da OAB pelo Distrito Federal (2010/2013 e 2019/2022) e Ouvidor-Geral Adjunto da OAB Nacional (2019/2022).

Fabrício da Mota Alves

Advogado especialista em Direito Digital. Tem vasta experiência na área, tendo participado ativamente no processo legislativo que levou à edição da Lei Geral de Proteção de Dados Pessoais brasileira. Coordenador jurídico da Frente Parlamentar de Proteção de Dados da Câmara dos Deputados. Representante do Senado Federal no Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, órgão que compõe a Autoridade Nacional de Proteção de Dados. Professor de Proteção de Dados em São Paulo (Insper, LEC, Escola Paulista de Direito e Opice Blum Academy), Distrito Federal (IDP e ATAME), Paraná (PUC), Rio de Janeiro (FGV) e Recife.

Ingo Wolfgang Sarlet

Advogado e parecerista. Doutor e Pós-Doutor em Direito pela Universidade de Munique. Professor Titular e Coordenador do Programa de Pós-Graduação em Direito da PUCRS. Desembargador aposentado do TJRS.
contato@ingosarlet.com.br

Mônica Tiemy Fujimoto

Professora do Instituto Brasiliense de Direito Público (IDP), Doutoranda e Mestre em Direito Empresarial e Econômico pela Universidade de Brasília (UnB) e graduada em direito pela Universidade de São Paulo (USP). Membra Consultora da Comissão Especial de Proteção de Dados Pessoais do Conselho Federal da OAB e Coordenadora de Relações Institucionais do Centro de Direito, Internet e Sociedade do IDP (CE-DIS/IDP). É sócia do escritório Horta e Bachur Advogados e é consultora da Laura Schertel Mendes Advocacia e Consultoria.

Tainá Aguiar Junquilho

Doutora em Direito pela Universidade de Brasília. Professora de Direito, tecnologia e inovação no IDP. Mestre em Direito pela UFES. Advogada.

AUTORES

Alisson A. Possa

Advogado, atualmente é Aluno Especial do Doutorado na Universidade de Brasília (UNB), Mestre em Direito Constitucial (IDP - Brasília), pesquisador internacional com estágio de pesquisa na Faculdad de Derecho de la Universidad de Granada (Espanha), Certified Informational Privacy Professional/Europe (CIPP/E - IAPP), possui treinamento profissional em proteção de dados pela Academy of European Law (ERA), pós-graduação em Direito Digital e Direito Processual Civil. Também é Membro da Comissão Especial de Direito Digital da OAB Nacional e Coordenador do Subcomitê de Acompanhamento Legislativo do GT de Proteção de Dados e IA da Frente Parlamentar do Setor de Serviços. Lattes:
http://lattes.cnpq.br/1795396755751129

Cacyone Gomes Barbosa Gonçalves Lavareda

Professora de Direito Digital e Proteção de Dados Pessoais, palestrante, advogada e jornalista. Mestre em Direito Constitucional pelo IDP (Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa); Data Protection Officer (DPO) pelo European Centre of Privacy and Cibersecurity (ECPC), Universidade de Maastricht (Holanda). Mestranda em Direito Civil na Faculdade de Direito do Recife (UFPE). Especialista em Direito Digital LLM Universidade Católica de Pernambuco (UNICAP). Pós-graduada em direito digital pela UNIDOMBOSCO. Pós-graduada em LGPD e GDPR pela Fundação Escola Superior do Ministério Público (FMP). DPO pela Academy of European Law (ERA-Germany). DPO pelo Instituto de Pesquisas Sociais, políticas e econômicas (IPESPE). Pesquisadora CEDIS / IDP PRIVACY LAB. Certificada pela IAPP / CIPM. Certificações pela L'université Paris Panthéon-Sorbonne, pela Dataprivacy Brasil, Exin, ABNT normas NBR ISO/IEC 27017 e 27018. Secretária da comissão de Proteção de Dados OAB/PE. Membro da Comissão Especial de Proteção de Dados do CFOAB.

Debora Sirotheau Siqueira Rodrigues

Advogada com pós-graduação em Privacidade e Proteção de Dados. Analista de TI com pós-graduação em Redes de Computadores. Certificada CIPM e CDPO/BR pela IAPP. Membro do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade- CNPD, órgão consultivo da Autoridade Nacional de Proteção de Dados - ANPD. Vice-presidente da Comissão Especial de Proteção de Dados da OAB Nacional. Presidente da Comissão Estadual de Proteção de Dados da OAB/PA. Conselheira Seccional da OAB/PA. Membro das Comissões de Relações Institucionais e de Relações do Trabalho do Instituto Nacional de Proteção de Dados – INPD.

Francisco Soares Campelo Filho

Francisco Soares Campelo Filho é Pós-Doutor em Direito e Novas Tecnologias pela Mediterranea International Centre for Human Rights Research da Università Mediterranea di Reggio Calabria - Itália. Doutor em Direito Público pela UNICEUB (DF). Mestre em Direito Público pela UNISINOS (RS). Membro Consultor da Comissão Especial de Proteção de Dados do Conselho Federal da OAB. Advogado.

Gabrielle Bezerra Sales Sarlet

Advogada e parecerista. Mestre em Direito pela UFC. Doutora em Direito pela Universidade de Augsburg. Pós-Doutorado em Direito pela Universidade de Hamburgo e pelo PPGD da PUCRS. Professora Adjunta da Escola de Direito da PUCRS nos níveis de graduação, mestrado e doutorado. Especialista em Neurociências pela PUCRS. gabriellebezerrasales@gmail.com

Ingo Wolfgang Sarlet

Advogado e parecerista. Doutor e Pós-Doutor em Direito pela Universidade de Munique. Professor Titular e Coordenador do Programa de Pós-Graduação em Direito da PUCRS. Desembargador aposentado do TJRS.
contato@ingosarlet.com.br

Jorge Alexandre Fagundes

Mestre em Negócios Internacionais pela Universidade de Ciência e Tecnologia de Miami - EUA, Advogado especialista em Direito Empresarial e digital, parecerista; Membro da ANADD - Associação Nacional dos Advogados de Direito Digital, Membro do Dtec – Estudos de Direito Digital e Proteção de Dados da Universidade Federal de Minas Gerais, UFMG; Coautor no livro Future Law, Vol. III, e Data Protection Officer (DPO), certificado pelo instituto Holandês EXIN na LGPD, no GDPR e nas ISO 27001/27002. DPO na OAB/ES, CRC/ES e no CRA/ES.

Lécio Silva Machado

Doutorando em Ciências Jurídicas Criminais em Coimbra Portugal; Mestre em Direito pela UNIFLU, Especialista em Direito Penal Econômico e Europeu pelo IDPEE, Coimbra, Portugal; Professor universitário, Advogado especialista em Direito digital e criminal, parecerista, escritor do livro "Comentários à Lei Geral de Proteção de Dados", editora Lumen Juris; Escritor do E-book "Lei Geral de Proteção de Dados aplicada às Igrejas", DPO na OAB/ES, CRC/ES e no CRA/ES.

Leide Jane Macedo da Silva

Advogada na área de Direito e Tecnologia e Empresarial. Data Protection Officer. Especialista em Direito e Tecnologia, Proteção de Dados para o setor público e privado e Cibersegurança. Professora de Especialização PUC Minas e cursos voltados para administração pública no IDCT - Instituto de Defesa da Cidadania e da Transparência. Diretora do Núcleo de Pesquisa e Extensão da Comissão de Proteção de Dados da OAB/MG.

Lucia Maria Teixeira Ferreira

Membra da Comissão Especial de Proteção de Dados do CFOAB. Coordenadora de Estudos e Pareceres da Comissão de Proteção de Dados e Privacidade da OAB/RJ. Doutoranda em Direito Constitucional no Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP). Mestre em Direito Civil pela Universidade do Estado do Rio de Janeiro (UERJ). Pós-Graduada em Sociologia Urbana pelo

Departamento de Ciências Sociais da UERJ. Professora e Membra da ABRADEP. Procuradora de Justiça aposentada do Ministério Público do Rio de Janeiro (MPRJ). Advogada. E-mail: luciaferreira@infolink.com.br. Currículo Lattes: http ://lattes.cnpq.br/8859827696202938.

Martha Leal

Advogada Especialista em Proteção de Dados. Advogada especialista em proteção de dados. Pós-graduada em Direito Digital pela Fundação Superior do Ministério Público do Rio Grande do Sul. Mestre em Direito e Negócios Internacionais pela Universidad Internacional Iberoamericana Europea del Atlântico e pela Universidad UNINI México. Pós-graduada em Direito Digital pela Universidade de Brasília - IDP. Data Protection Officer ECPB pela Maastricht University. Certificada como Data Protection Officer pela EXIN. Certificada como Data Protection Officer pela Fundação Getúlio Vargas do Rio de Janeiro - FGV. Mestranda na Unisinos – Mestrado Profissional em Direito. Presidente da Comissão de Comunicação Institucional do Instituto Nacional de Proteção de Dados – INPD. E-mail: marta@jpleal.com.br.

Melissa Barrioni e Oliveira

Presidente da Comissão de Proteção de Dados da OAB/MG - triênio 2022/2024. Membro Consultora da Comissão Especial de Proteção de Dados do CFOAB. Professora e Coordenadora da Pós-graduação em de Proteção de Dados e Privacidade da ESA/MG e CEDIN. Palestrante. Especializada em Compliance e LGPD. Partner e Co-founder da BSS Consult. Pós-Graduada em Direito do Trabalho e Processo do Trabalho pelo CAD (Centro de Atualização em Direito) e FUMEC/MG. Pós-Graduada em Docência com Ênfase em Educação Jurídica pela Universidade Arnaldo.

Rebeca Azevedo

Mestranda em Direito Constitucional Acadêmico no Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP). Possui graduação em Direito (2018) e Pós-Graduação em Prática Processual (2022), ambos pelo Centro

Universitário de Brasília - UniCEUB. Advoga desde 2019 na Advocacia Fernanda Fernandez, com foco nos Tribunais Superiores, no Tribunal Regional Federal da 1ª Região e na Justiça Federal do Distrito Federal. Sua expertise está voltada para o Direito Público, com ênfase em Direito Constitucional, Tributário e Administrativo. Além disso, é membra da Comissão de Precatórios da OAB/DF e recebeu reconhecimento por suas contribuições no campo jurídico, incluindo menções em publicações renomadas como The Legal 500, nos anos de 2023 e 2024. Lattes: http://lattes.cnpq.br/6006779308971461

Stella Muniz Campos Elias

Advogada Empresarial. Mestra pelo Programa de Pós-Graduação *stricto sensu* em Direito da Pontifícia Universidade Católica de Minas Gerais – PUC Minas. Pós-Graduada em Direito do Trabalho e Processo do Trabalho pela Pontifícia Universidade Católica de Minas Gerais – PUC Minas. Pós-graduada em Docência com Ênfase Jurídica. Consultora e Especialista em Proteção de Dados. Consultora e Especialista em Proteção Trabalhista. Membro consultora da Comissão Especial de Proteção de Dados da OAB Nacional. Vice-presidente da Comissão de Proteção de Dados da OAB/MG. Membro do Programa e da Comissão do Direito na Escola. Membro da Comissão de Direitos Sociais e Trabalhistas da OAB/MG. Membro do Grupo de Pesquisa e Extensão Capitalismo e Proteção Social na Perspectiva dos Direitos Humanos e Fundamentais do Trabalho e da Seguridade Social. E-mail:
contato@stellacampos.com.br

SUMÁRIO

APRESENTAÇÃO

Prezados Leitores,

É com grande satisfação que a Comissão Especial de Proteção de Dados (CEPD) e a Comissão Especial de Direito Digital (CEDD) do Conselho Federal da OAB apresentam o anuário com o tema "Direitos Fundamentais na Era Digital". Este projeto reflete o compromisso das nossas comissões com a promoção do conhecimento, bem como o incentivo à produção acadêmica e científica no campo da proteção de dados pessoais e direito digital, alinhado com nossos objetivos institucionais.

A escolha do tema "Direitos Fundamentais na Era Digital" é uma forma de prestar uma homenagem e um tributo ao saudoso Professor e Advogado Danilo César Maganhoto Doneda, cuja contribuição inestimável para o debate sobre a efetividade dos princípios constitucionais na era digital é indiscutível. Sua obra de 2006, "Da Privacidade à Proteção de Dados Pessoais", foi pioneira no debate sobre proteção de dados no Brasil, reconhecendo há muito tempo a importância da tutela constitucional relacionada à proteção de dados pessoais.

Por meio de sua pesquisa de excelência, perspectiva humanista e compromisso com a garantia dos direitos humanos, Danilo inspirou fortemente a construção do marco regulatório no Brasil, tornando-se uma figura central nas principais discussões sobre cidadania digital no país. Ele foi membro indicado pela Câmara dos Deputados para o Conselho Nacional de Proteção de Dados e Privacidade, participou das discussões sobre a elaboração do Marco Civil da Internet, foi coautor do anteprojeto da LGPD, integrou a Comissão de Juristas responsável pelo anteprojeto da LGPD Penal e a Comissão de Juristas (CJSUBIA) responsável por subsidiar a elaboração da minuta do substitutivo sobre inteligência artificial no Brasil. Sua relevância ultrapassou as fronteiras do Brasil, sendo o primeiro brasileiro a ser nomeado diretor da *International Association of Privacy Professionals* (IAPP), participando de importantes fóruns de discussão em todo o mundo e publicando artigos relevantes em grandes veículos acadêmicos.

Na advocacia, Danilo teve uma participação relevante na Ação Direta de Inconstitucionalidade nº 6389, relativa à inconstitucionalidade do art. 2º, caput e §§

1º e 3º da Medida Provisória 954/2020, cujo julgamento culminou no reconhecimento da existência de um direito fundamental autônomo à proteção de dados pessoais. Além disso, desempenhou um papel central no julgamento da Ação Direta de Inconstitucionalidade nº 6649, que trata do compartilhamento de dados pessoais entre órgãos e entidades da administração pública federal, e apresentou pareceres em diversos debates relevantes no sistema judiciário brasileiro.

O anuário está dividido em duas partes distintas e complementares. A Parte 1 concentra-se nos trabalhos das Comissões Especiais de Direito Digital e de Proteção de Dados, com a colaboração de coautores externos, e apresenta uma seleção de artigos que analisam os desafios e as implicações da era digital nos direitos fundamentais.

Os temas abordados na Parte 1 são de notável relevância e englobam debates importantes como a ameaça da inteligência artificial ao devido processo legal, o contexto da Lei Geral de Proteção de Dados Pessoais no cenário brasileiro, o empoderamento do indivíduo por meio do sistema europeu de proteção de dados, o equilíbrio entre o direito fundamental à proteção de dados pessoais e o uso da inteligência artificial, bem como a separação informacional de poderes no compartilhamento de dados pessoais. Além disso, exploramos o papel da Autoridade Nacional de Proteção de Dados Pessoais (ANPD) na proteção do direito fundamental à proteção de dados pessoais, a proteção multinível dos dados pessoais como um direito internacional humano e as implicações dos julgamentos envolvendo a separação informacional de poderes e os limites do compartilhamento de dados pessoais.

A Parte 2 é dedicada exclusivamente à obra do nosso querido Danilo Doneda. Seu legado é celebrado nesta seção, que destaca seu profundo conhecimento e contribuições cruciais para o campo dos direitos fundamentais na era digital. Nessa parte, contamos com a transcrição das suas sustentações orais no julgamento das históricas Ações Diretas de Inconstitucionalidade nº 6389 e 6649, além de dois importantes artigos sobre a proteção de dados como um direito fundamental.

O anuário "Direitos Fundamentais na Era Digital" é um trabalho que visa contribuir para o importante debate sobre as diversas esferas de direitos, liberdades e garantias que estão sendo revistas e redefinidas no contexto das transformações

digitais em constante evolução. Esperamos que esta obra seja um instrumento valioso na disseminação do conhecimento e na formação de profissionais capacitados nessa área.

Agradecemos a todos os envolvidos e esperamos que este anuário seja uma homenagem digna ao legado do Professor Danilo Doneda, que tanto contribuiu para o avanço do entendimento e da prática no campo dos direitos fundamentais na era digital. E agradecemos, especialmente, à Revista Espaço Jurídico, na pessoa de seu editor-chefe, Wilson Steinmetz, e à Revista de Direito do Consumidor, na pessoa de sua Coordenadora Claudia Lima Marques, por terem autorizado a republicação dos artigos do Danilo que inicialmente foram disponibilizados em suas publicações.

PREFÁCIO

Esta coletânea reúne textos constituídos a partir das experiências de juristas com referência no campo do direito digital e da proteção de dados. Muitos de seus autores e autoras compõem da Comissão Especial de Direito Digital e a Comissão Especial de Proteção de Dados de Proteção de Dados - presididas, respectivamente, pela dra. Laura Schertel e pelo dr. Rodrigo Badaró. Ambas são essenciais para as discussões sobre os desafios jurídicos apresentados pelos avanços tecnológicos.

Essas Comissões Especiais brindam a comunidade jurídica brasileira com uma obra coletiva instigante, dividida em duas grandes partes. A primeira destina-se ao estudo específico da proteção de dados, desde a sua consolidação no sistema europeu ao desenvolvimento do conceito no ordenamento brasileiro. A segunda diz respeito às atuais discussões que permeiam o constitucionalismo digital, incluindo os *hard cases* decorrentes do uso de Inteligência Artificial e algoritmos pelos operadores do direito, bem como os impactos para a democracia.

A Lei Geral de Proteção de Dados Pessoais (LGPD), fruto de um processo legislativo democrático, foi criada para conferir segurança jurídica ao tratamento de dados pessoais no Brasil. Com vasto conhecimento da prática jurídica e da doutrina do direito comparado, a advocacia nacional – sob liderança das duas comissões especiais – orientou o Poder Legislativo a adotar o conceito de "autodeterminação informativa"[1]. Assim, o ordenamento brasileiro passou a tratar os dados pessoais como uma ramificação do direito constitucional da personalidade.

Em 2022, a Emenda Constitucional (EC) nº 115 assegurou "o direito à proteção de dados" como garantia fundamental. A previsão constitucional reforçou os princípios da LGPD e destacou a ideia de que os dados pessoais são relevantes e só podem ter utilizados pela iniciativa privada ou pelo Poder Público diante da demonstração de interesse legítimo.

Composta por artigos científicos e comentários de jurisprudência dos membros da comissão e coautores externos, esta coletânea traz a excelência do

---

[1] Princípio fundamental da Lei de Proteção de Dados, constante no seu art. 2, II, que se traduz na faculdade de o particular determinar e controlar a utilização de seus dados. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

debate realizado na OAB, além de homenagear o saudoso dr. Danilo Doneda. Advogado brilhante, mestre e doutor pela Universidade do Estado do Rio de Janeiro (UERJ), coordenou a redação do anteprojeto da LGPD e sua presença foi crucial para os avanços e desafios abordados neste livro. Ainda jovem, consagrou-se como autoridade no tema sobre proteção de dados no início da carreira. Publicou obras basilares para todo e qualquer estudante de direito. Foi reconhecido internacionalmente por sua atuação. Este livro é uma homenagem ao seu pensamento atemporal e às suas contribuições para o direito e para a advocacia.

A pluralidade é o símbolo central desta obra. Sua relevância amplia o público-alvo. Abrange tanto os profissionais do direito iniciantes como os mais experientes na área. Por isso, é digno de nota o trabalho impecável da coordenação e da organização dos estimados Dr. Rodrigo Badaró e Dra. Laura Schertel Mendes, os quais reuniram grandes autores e autoras que compõem este livro.

A coletânea nasce como uma grande referência para refletir e propor novos rumos para o direito e, em especial, para a interlocução do Direito Digital e da Proteção de Dados com o Direito Constitucional, Direito Internacional e Direito Comparado. Os textos conversam e interagem entre si com uma excelência de argumentos científicos e teórico-práticos. Esta peculiaridade possibilita a qualificação de debates importantes para a sociedade brasileira e global, sobretudo com a emergência das discussões sobre regulação da Inteligência Artificial e a relação entre digitalização, democracia e direitos fundamentais.

O presente livro contribui, portanto, para o aperfeiçoamento do sistema jurídico, cumprindo o papel institucional da advocacia, que é, conforme o mandamento constitucional, indispensável à Justiça. Trata-se de material essencial para todas e todos aqueles que se dedicam à advocacia e à consolidação do Estado Democrático de Direito em nosso País.

Boa leitura!

José Alberto Simonetti[2]

[2] Advogado. Presidente do Conselho Federal da Ordem dos Advogados do Brasil (CFOAB).

PARTE 1 – TRABALHOS DA COMISSÃO ESPECIAL DE DIREITO DIGITAL E DA COMISSÃO ESPECIAL DE PROTEÇÃO DE DADOS

1. A AMEAÇA DA INTELIGÊNCIA ARTIFICIAL AO DEVIDO PROCESSO LEGAL: UMA ANÁLISE SOBRE AS GARANTIAS PROCESSUAIS NO DESENVOLVIMENTO DE NOVAS TECNOLOGIAS PELO JUDICIÁRIO BRASILEIRO

https://doi.org/10.36592/9786554600798-01

Alisson A. Possa[1]
Rebeca Azevedo[2]

RESUMO
O Poder Judiciário do Brasil está passando por uma revolução digital com centenas de projetos para desenvolvimento e implementação de tecnologias de Inteligência Artificial para melhorar a produtividade dos servidores e acelerar o tempo de tramitação de processos judiciais. A Resolução 332 de 2020 do Conselho Nacional de Justiça regulamenta esses projetos, indicando requisitos e estabelecendo mecanismos de controle. Ocorre que há deficiências graves na regulamentação ao não estabelecer critérios que observem as garantias do devido processo legal e a participação de agentes que não sejam membros do Poder Judiciário na etapa de desenvolvimento. Esses problemas podem gerar severos danos sociais através da violação das garantias aos jurisdicionados.
Palavras-chave: Devido Processo Legal; Inteligência Artificial; Conselho Nacional de Justiça;

Introdução

A digitalização da justiça brasileira permitiu avanços no desenvolvimento de tecnologias classificadas como inteligência artificial para acelerar o funcionamento

[1] Advogado, atualmente é Aluno Especial do Doutorado na Universidade de Brasília (UNB), Mestre em Direito Constitucional (IDP - Brasília), pesquisador internacional com estágio de pesquisa na Faculdad de Derecho de la Universidad de Granada (Espanha), Certified Informational Privacy Professional/Europe (CIPP/E - IAPP), possui treinamento profissional em proteção de dados pela Academy of European Law (ERA), pós-graduação em Direito Digital e Direito Processual Civil. Também é Membro da Comissão Especial de Direito Digital da OAB Nacional e Coordenador do Subcomitê de Acompanhamento Legislativo do GT de Proteção de Dados e IA da Frente Parlamentar do Setor de Serviços. Lattes: http://lattes.cnpq.br/1795396755751129
[2] Mestranda em Direito Constitucional Acadêmico no Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP). Possui graduação em Direito (2018) e Pós-Graduação em Prática Processual (2022), ambos pelo Centro Universitário de Brasília - UniCEUB. Advoga desde 2019 na Advocacia Fernanda Fernandez, com foco nos Tribunais Superiores, no Tribunal Regional Federal da 1ª Região e na Justiça Federal do Distrito Federal. Sua expertise está voltada para o Direito Público, com ênfase em Direito Constitucional, Tributário e Administrativo. Além disso, é membra da Comissão de Precatórios da OAB/DF e recebeu reconhecimento por suas contribuições no campo jurídico, incluindo menções em publicações renomadas como The Legal 500, nos anos de 2023 e 2024. Lattes: http://lattes.cnpq.br/6006779308971461

do judiciário no país. A mudança de documentos em papel para o formato eletrônico permite que diversas informações sejam inferidas a partir de seu conteúdo e metadados. Com ferramentas adequadas, essas informações podem ser extraídas em grandes quantidades, classificadas e posteriormente utilizadas para gerar novas inferências ou servir de base para o treinamento de outros sistemas informacionais.

Desde então, munidos de bases de dados imensas que derivam da grande quantidade de processos judiciais no país, os Tribunais passaram a olhar para tecnologias que permitam acelerar o tempo de tramitação processual e facilitar tarefas para os servidores. Atualmente, segundo a Plataforma Sinapses do Conselho Nacional da Justiça, existem 53 Tribunais com Projetos de IA, em um total de 111 projetos[3], sendo o projeto VICTOR do Supremo Tribunal Federal o primeiro a ser utilizado, desde 2017[4].

Nesse contexto, questões sobre o desenvolvimento ético passaram a pautar diversas discussões sobre essas implementações, principalmente acerca de vieses discriminatórios, transparência algorítmica, impactos sobre os cidadãos, entre outras.

Dentre os questionamentos de ordem ética ou impactos negativos diretamente aos cidadãos, chama atenção um ponto específico: a compatibilidade das garantias que compõem o direito ao devido processo legal e a implementação de sistemas que não somente automatizam etapas processuais, mas também estão passando a classificar, analisar conteúdo e, quem sabe futuramente, até mesmo sugerir decisões completas.

Diante da temática supramencionada, o presente artigo busca responder à pergunta: É possível conciliar a garantia do devido processo legal com a implementação da Inteligência Artificial no Judiciário Brasileiro?

Para responder esse questionamento, no primeiro item será avaliado o presente contexto de desenvolvimento e usos de inteligências artificiais para os

---

[3] A plataforma permite o acompanhamento em tempo real, indicando que houve um aumento de 171% em relação à 2021. Disponível em https://paineisanalytics.cnj.jus.br/single/?appid=9e4f18ac-e253-4893-8ca1-b81d8af59ff6&sheet=b8267e5a-1f1f-41a7-90ff-d7a2f4ed34ea&lang=pt-BR&theme=IA_PJ&opt=ctxmenu,currsel&select=language,BR . Acesso em: 11 de set de 2023.

[4] Conforme relatado pelo próprio STF. Disponível em:[https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=499690&ori= . Acesso em 06 de setembro de 2023.

processos judiciais, e os potenciais riscos envolvidos e problemas já apontados na literatura nacional e internacional.

Em seguida será estudado o conteúdo normativo do direito ao devido processo legal, analisando o atual estado da arte jurisprudencial e legal sobre esse direito.

Por fim, será analisado o presente cenário regulatório existente e como salvaguardas ainda não previstas, mas que decorrem do direito ao devido processo legal, podem ser implementadas pelos Tribunais para o desenvolvimento dessas tecnologias em linha com as garantias constitucionais e processuais analisadas.

1. O desenvolvimento de IAs no Judiciário

As possibilidades de utilização das tecnologias de inteligência artificial no Direito são várias. Tainá Aguiar Junquilho sistematiza os seguintes usos:

Tabela 1 – IAs no Direito

Aprendizado em máquina	Usados no Direito para:	Artigos CPC/15
Modelos preditivos	*Legal analytics/* Jurimetria, "fórum shopping", ODR, identificação de fraudes, elaboração de alertas e criação de indicadores/métricas	Arts. 63 e 926
Organização de documentos	Agrupamento, triagem e classificação de processos e peças; automação de rotinas internas aos tribunais e escritórios	Art. 8º
Busca textual	Buscadores de jurisprudências similares	Art. 926 e seguintes
Automação de documentos	Geração automática de peças por transcrição de voz	Art. 8°

	para texto ou com base em documentos anteriores escritos	
Decisões automatizadas	Apoio à tomada de decisões; ou criação de sentenças, despachos e decisões jurídicas em geral.	Art. 489

Fonte: JUNQUILHO, Tainá Aguiar. Inteligência Artificial no Direito – Limites Éticos. São Paulo: Juspodivm, 2022, p. 83-84

Referidas funcionalidades estão dentro do escopo total de atividades que fazem parte das profissões jurídicas, incluindo escritórios de advocacia.

Desses possíveis usos, especificamente no Judiciário, Tania Sourdin sistematiza em três níveis:

> First, and at the most basic level, technology is assisting to inform, support and advise people involved in the justice system (supportive technology). Second, technology can replace functions and activities that were previously carried out by humans (replacement technologies). Finally, at a third level, technology can change the way that judges work and provide for very different forms of justice (disruptive technology), particularly where processes change significantly and predictive analytics may reshape the adjudicative role[5]

Tal categorização tem como critério o papel que a IA pode desempenhar junto aos Tribunais: desde a inferência de informações sobre um determinado documento até a análise preditiva para possíveis decisões.

---

[5] Em primeiro lugar, e ao nível mais básico, a tecnologia ajuda a informar, apoiar e aconselhar as pessoas envolvidas no sistema judicial (tecnologia de apoio). Em segundo lugar, a tecnologia pode substituir funções e atividades que anteriormente eram realizadas por seres humanos (tecnologias de substituição). Finalmente, num terceiro nível, a tecnologia pode mudar a forma como os juízes trabalham e proporcionar formas muito diferentes de justiça (tecnologia disruptiva), particularmente onde os processos mudam significativamente e a análise preditiva pode remodelar o papel jurisdicional. (Tradução nossa). Cf SOURDIN, Tania. Judge v Robot?: Artificial intelligence and judicial decision-making. **University of New South Wales Law Journal, The**, v. 41, n. 4, p. 1114-1133, 2018, p. 1117

No âmbito do Poder Judiciário, todas essas possibilidades podem acarretar prejuízos ao devido processo legal, ainda que em procedimentos de suporte, principalmente na falta de transparência sobre a participação das IAs e a relação do ser humano quando conscientemente apoiado por algoritmos.

Um exemplo possível é a classificação incorreta de um caso em uma determinada categoria de processos que pode trazer consequências negativa à uma das partes. Ainda que servidores ou juízes sejam responsáveis por validar os efeitos jurídicos decorrentes da mencionada classificação, é de notório conhecimento que o grande acervo de processos pode levar à falta de uma análise crítica do ser humano sobre a indicação da tecnologia, convalidando consequências que atentam contra direitos das partes.

Outro exemplo a ser citado são os buscadores de textos, que podem ser utilizados para que o julgador utilize decisões na sua fundamentação e que, dependendo de como os critérios para seu treinamento foram utilizados, podem acabar indicando aquelas que reforçam uma determinada posição jurisprudencial – o que, por vezes, não se adequa ao caso concreto.

Isso porque, pela própria arquitetura de como resultados podem ser exibidos (pensando, por exemplo, em como buscadores como Google posicionam alguns resultados na primeira página em evidência e o usuário dificilmente navegue além das primeiras posições), pode-se reforçar o uso de interpretações e aplicações de precedentes, sem que o julgador considere a existência de divergências e ressalvas incidentes sobre determinados pleitos. Ou seja, sem o devido cotejo analítico e observância das especificidades de cada processo.

Ainda que esse problema já seja possível com as atuais ferramentas de busca de jurisprudências, a existência de um algoritmo que, na teoria, é neutro e vai corresponder às demandas do usuário com mais acurácia que os buscadores sem essas tecnologias, pode acabar por violar garantias ao reforçar determinadas posições jurisprudenciais sem levar em conta o caso concreto.

Alguns dos maiores riscos estão nas tecnologias das análises preditivas, que podem ser utilizadas como suporte ou em conjunto com a automação de decisões judiciais. O caso mais famoso até então é *Correctional Offender Management Profiling for Alternative Sanctions* (COMPAS) nos Estados Unidos, no qual uma IA foi

utilizada para avaliar o histórico criminal e indicar a possibilidade de reincidência do indivíduo, a fim de auxiliar juízes criminais no momento de decidir acerca da prisão[6]. Objeto de questionamento no caso *State v Loomis*, a decisão da Suprema Corte de Wisconsin foi debatida pelos parâmetros na utilização de análises preditivas sobre comportamentos individuais pelo Judiciário, sendo alvo de críticas sobre questões como discriminação algorítmica, viés racial, entre outros problemas. Importante destacar que, nesse caso, o COMPAS foi caracterizado como uma ferramenta para auxiliar o julgador, e não deveria ser levado em conta como o único elemento para a decisão[7].

No Brasil, um exemplo de IA com análise preditiva utilizado como suporte para ações humanas é o sistema IRIS, empregado pela Receita Federal, que utiliza reconhecimento facial biométrico e combina com os dados de voo do passageiro (meio de compra do bilhete, tempo de voo, peso da bagagem, moeda utilizada) e dados provenientes da Polícia Federal para classificar viajantes em grupos e indicar uma probabilidade de o passageiro estar cometendo uma infração tributária permitindo que o agente aduaneiro humano seja alertado sobre a necessidade de fiscalizar o indivíduo[8].

Ainda, um dos usos mais polêmicos é a possibilidade de automação de decisões judiciais por algoritmos. Considerando que a grande quantidade de processos na Justiça brasileira, metas e o clamor popular por mais celeridade nos julgamentos, a possibilidade de algoritmos criarem decisões em milésimos de segundos acaba por ser um argumento sedutor a favor desses usos. As discussões acabam por ser sobre em quais áreas e tipos de processos essa substituição do julgador pela máquina pode ser realizada[9] ou se a IA deve estar limitada a gerar

---

[6] LIU, Han-Wei; LIN, Ching-Fu; CHEN, Yu-Jie. Beyond State v Loomis: artificial intelligence, government algorithmization and accountability. **International journal of law and information technology**, v. 27, n. 2, p. 122-141, 2019, p. 6-7

[7] *Ibidem*, p. 7-8

[8] ALBUQUERQUE, Adriana. PODER ARTIFICIAL DE TRIBUTAR – LIMITES E REQUISITOS À UTILIZAÇÃO (ADEQUADA) DA INTELIGÊNCIA ARTIFICIAL PELA ADMINISTRAÇÃO TRIBUTÁRIA. Londrina: Toth, 2023, p. 48-49.

[9] São exemplos de SIQUEIRA, MORAIS E SANTOS os "despachos repetitivos, decisões repetitivas, sentenças padrões, ou decisões monocráticas de relator, a exemplo, respectivamente, do despacho que determina a citação inicial em execução fiscal, da decisão que determina a penhora on-line de ativos financeiros, da sentença de extinção do processo por pagamento ou desistência ou da decisão monocrática de relator que julga prejudicado o agravo de instrumento face à sentença exarada pelo juiz de primeiro grau". SIQUEIRA, Dirceu Pereira; MORAIS, Fausto Santos de; SANTOS, Marcel Ferreira

possibilidades de decisões que o magistrado poderá complementar, tal como atividades cotidianas de assessores e estagiários.

Perante a garantia do devido processo legal, todas as utilizações de IAs apontadas acima trazem diversas possibilidades de danos, desde as mais sutis que derivam de erros dos indicadores de acuraria dos algoritmos que podem ser validados por servidores do Judiciário, até questões mais complexas como a influência que o resultado do uso dessas tecnologias pode ter nos rumos do processo.

É nesse contexto que os estudos sobre "efeito âncora" de algoritmos no processo cognitivo de julgadores e outros servidores apontam os tipos de situações que colocam em risco o direito ao devido processo legal. Essa relação é indicada por LIU, LIN e CHEN quando da crítica sobre a análise da Suprema Corte de Wisconsin que indicou o COMPAS como um elemento adicional a ser levado em conta no processo de convicção do julgador:

> That is, the Court failed to consider the psychological 'anchoring effect' for courts using scientific and technological tools, as numerous studies have demonstrated how judges (and human individuals) are submissive to computer-generated numbers and results that may further frame and condition the view of judges. Mere written warnings do not seem to be able to adequately inform judges as effective gatekeepers, especially when they may not be sufficiently equipped with expertise as to understand the workings of such tools[10](grifo nosso)

Esse efeito pode ser um problema adicional no procedimento decisório dos julgadores, objeto de amplo debate no Brasil diante de críticas às expressões como

---

dos. Inteligência artificial e jurisdição: dever analítico de fundamentação e os limites da substituição dos humanos por algoritmos no campo da tomada de decisão judicial. **Sequência (Florianópolis)**, v. 43, 2023, p. 16

[10] "Ou seja, o Tribunal não considerou o "efeito de ancoragem" psicológico para os tribunais que utilizam ferramentas científicas e tecnológicas, uma vez que numerosos estudos demonstraram como os juízes (e os indivíduos humanos) são submissos a números e resultados gerados por computador que podem enquadrar e condicionar ainda mais a visão dos juízes. Meras advertências escritas não parecem ser capazes de informar adequadamente os juízes como guardiões eficazes, especialmente quando eles podem não estar suficientemente equipados com conhecimentos especializados para compreender o funcionamento de tais ferramentas" (tradução nossa). LIU, LIN, CHEN, *op. cit*, p. 9

o “livre convencimento motivado”[11] e a obrigação constitucional da fundamentação de decisões judiciais (art. 93, inciso IX da Constituição Federal).

O agravamento de problemas polêmicos na jurisdição brasileira pode decorrer da mera reprodução dos resultados indicados por algoritmos sem que o julgador necessariamente analise os possíveis erros e omissões perante o contexto processual (que, diga-se de passagem, é uma situação infelizmente já comum sem o uso de tecnologias), valendo-se de uma concepção psicológica de que os sistemas tecnológicos realizam atividades com maior assertividade de que os humanos.

É no presente contexto que o principal objeto desse artigo está inserido: buscar identificar parâmetros para como as inteligências artificiais no Judiciário podem ser implementadas sem agravar ou criar violações à garantia do devido processo legal.

No próximo item realizamos um estudo do direito ao devido processo legal para, posteriormente, verificar como o atual cenário regulatório prevê os elementos que o caracterizam e identificar melhorias que podem ser implementadas.

2. O devido processo legal no Brasil

O princípio do Devido Processo Legal representa um dos alicerces fundamentais do Estado Democrático de Direito. Encontra-se expressamente consagrado no artigo 5º, inciso LIV, da Constituição Federal[12], e tem por escopo garantir que o indivíduo somente seja privado de sua liberdade ou tenha seus direitos restringidos por meio de um procedimento legal, conduzido pelo Poder Judiciário, sob a égide de um juiz natural. Ele visa garantir que as partes não sejam lesadas com práticas não especificadas e que aquelas estejam de acordo com a lei vigente.

Existe uma certa dificuldade em definir o conceito de devido processo legal, dentre outras razões, por sua vagueza e amplitude em muitas vezes indeterminada[13].

---

[11] Um dos críticos a esse instituto é Lênio Streck. Ver STRECK, Lenio Luiz. Dicionário de hermenêutica: 50 verbetes fundamentais da teoria do direito à luz da crítica hermenêutica do direito. 2. ed. Belo Horizonte: Casa do direito, 2020.

[12] “LIV - ninguém será privado da liberdade ou de seus bens sem o devido processo legal;”

[13] DINAMARCO, Cândido Rangel. Instituições de Direito Processual Civil. 7 ed. São Paulo: Malheiros Editores, 2015, v. 1, p. 250.

A tradução para o português de "Devido Processo Legal" corresponde à expressão inglesa "*due process of law*". Todavia, "*law*" no seu significado de "direito", e não somente de lei. Tal observação é importante pois significa dizer que o processo há de estar em conformidade com o Direito como um todo, e não apenas em consonância com a lei[14].

Para Luiz Fux, em razão dessa dupla conotação (lei justa e processo judicial justo) o princípio do devido processo legal tem como um dos seus fundamentos o processo "justo", que é aquele adequado às necessidades de definição e realização dos direitos lesados[15]. No mesmo sentido, de acordo com o entendimento de José Baracho, "o direito de ação e o direito de defesa judicial são assegurados aos indivíduos, de modo completo, por toda uma série de normas constitucionais que configuram o que se denomina de '*due process of law*', processo que deve ser justo e leal"[16].

Pela relevância do tema, o referido princípio também encontra previsão no inciso 1º do art. 8º, da Convenção Americana de Direitos Humanos (Pacto de São José da Costa Rica)[17], *verbis:*

> Artigo 8º - Garantias judiciais: 1. Toda pessoa terá o **direito de ser ouvida**, com as devidas garantias e **dentro de um prazo razoável**, por um **juiz ou Tribunal competente**, **independente e imparcial**, estabelecido anteriormente **por lei**, na apuração de qualquer acusação penal formulada contra ela, ou na determinação de seus direitos e obrigações de caráter civil, trabalhista, fiscal ou de qualquer outra natureza.(grifos nossos).

Daí é de se perceber que o conceito do devido processo legal abrange uma série de normas, garantias processuais e preceitos constitucionais que consagram tanto o direito de ação quanto o direito de defesa. De acordo com José Afonso da

---

[14] DIDIER JUNIOR, Fredie. Curso de direito processual civil: introdução ao direito processual civil e processo de conhecimento. 13. ed. Salvador: Juspodivm, 2011. v. 1, p. 45.
[15] FUX, Luiz. Curso de Direito Processual Civil. 5ª Edição. Rio de Janeiro: Forense, 2022, p. 38-39
[16] BARACHO, José Alfredo Oliveira. Processo Constitucional. In: ____. Direito processual constitucional: aspectos contemporâneos. [s.n.t.]. p. 67.
[17] CONVENÇÃO Americana de Direitos Humanos. 22 de nov de 1969.

Silva, esse princípio combinado com o direito de acesso à justiça (artigo 5º, XXXV)[18], o contraditório e a ampla defesa (art. 5º, LV)[19], fecha o ciclo das garantias processuais. Dessa forma, garante-se o processo, com as formas instrumentais adequadas, de forma que a prestação jurisdicional, quando entregue pelo Estado, dê a cada um, o que é seu[20].

De fato, o contraditório, a ampla defesa e o direito de acesso à justiça (princípio da inafastabilidade da jurisdição) dizem respeito ao devido processo legal. Todavia, na prática percebemos que materialização do devido processo legal se dá de forma ainda mais abrangente e, em razão disso para se ter a concretização daquele princípio é necessário observar, também: **(a)** a publicidade do processo (art. 5º, LX, CF)[21]; **(b)** a proibição da produção de provas ilícitas (art. 5º, LVI)[22]; **(c)** a imparcialidade do julgador, bem como a garantia do juiz natural (art. 5º, XXXVII[23] e LIII[24]); **(d)** a motivação das decisões (art. 93, IX)[25]; **(e)** a duração razoável do processo (art. 5º, LXXVIII)[26], **(f)** o tratamento paritário conferido às partes envolvidas no processo (art. 7º, CPC/2015)[27]; dentre outros.

Assim sendo, considerando a complexidade da natureza e extensão do conteúdo do princípio do devido processo legal, é apropriado oferecer alguns comentários sobre as exigências retromencionadas, as quais desempenham um papel crucial na concretização do princípio em análise.

---

[18] XXXV - a lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito;
[19] LV - aos litigantes, em processo judicial ou administrativo, e aos acusados em geral são assegurados o contraditório e ampla defesa, com os meios e recursos a ela inerentes
[20] SILVA, José Afonso da. **Curso de direito constitucional positivo**. 25. ed. rev. e atual. São Paulo: Malheiros, 2005. p. 431-432.
[21] LX - A lei só poderá restringir a publicidade dos atos processuais quando a defesa da intimidade ou o interesse social o exigirem;
[22] LVI - são inadmissíveis, no processo, as provas obtidas por meios ilícitos;
[23] XXXVII- não haverá juízo ou tribunal de exceção
[24] LIII - ninguém será processado nem sentenciado senão pela autoridade competente;
[25] IX - todos os julgamentos dos órgãos do Poder Judiciário serão públicos, e fundamentadas todas as decisões, sob pena de nulidade, podendo a lei limitar a presença, em determinados atos, às próprias partes e a seus advogados, ou somente a estes, em casos nos quais a preservação do direito à intimidade do interessado no sigilo não prejudique o interesse público à informação;
[26] LXXVIII - a todos, no âmbito judicial e administrativo, são assegurados a razoável duração do processo e os meios que garantam a celeridade de sua tramitação.
[27] Art. 7º É assegurada às partes paridade de tratamento em relação ao exercício de direitos e faculdades processuais, aos meios de defesa, aos ônus, aos deveres e à aplicação de sanções processuais, competindo ao juiz zelar pelo efetivo contraditório".

Relativamente ao princípio do contraditório, este, em resumo, representa a oportunidade de resposta. É "entendido como a ciência bilateral dos atos do processo com a possibilidade de contrariá-los, é composto por dois elementos: informação e reação, sendo esta meramente possibilitada em se tratando de direitos disponíveis"[28].

A ampla defesa, por sua vez, caminha juntamente com o princípio do contraditório, a fim de assegurar ao indivíduo o seu direito de defesa em todas as fases do processo. E é assim que vemos a aplicação desses princípios perante o judiciário brasileiro. Destacamos, à título exemplificativo:

> "AGRAVO REGIMENTAL EM RECURSO EXTRAORDINÁRIO. CONSTITUCIONAL. ADMINISTRATIVO. SERVIDOR PÚBLICO NÃO ESTÁVEL. DEMISSÃO. NECESSIDADE DE OBSERVÂNCIA DE **CONTRADITÓRIO** E **AMPLA DEFESA.** I - A demissão de servidor público, mesmo que não estável, deve ser precedida por processo administrativo, **em que sejam assegurados o contraditório e a ampla defesa**. Precedentes. II - Agravo regimental não provido. (grifos nossos)[29]

Ainda a despeito dos princípios do contraditório e ampla defesa, é de se destacar o teor da Súmula Vinculante n. 3 do STF, segundo a qual:

> Nos processos perante o Tribunal de Contas da União asseguram-se o contraditório e a ampla defesa quando da decisão puder resultar anulação ou revogação de ato administrativo que beneficie o interessado, excetuada a apreciação da legalidade do ato de concessão inicial de aposentadoria, reforma e pensão"[30].

Em relação à publicidade, estatuída no mencionado inciso LX, do art. 5º, da CF[31] é de se verificar que tal princípio é fonte de legitimidade e garantia de controle

---

[28] CUNHA JÚNIOR, Dirley da; NOVELINO, Marcelo. **Constituição Federal para concursos**. 2. ed. rev., ampl. e atual. Salvador: Juspodivm, 2011. p. 93.

[29] BRASIL. Supremo Tribunal Federal. **Agravo Regimental no Recurso Extraordinário 594.040.** Relator: Min. Ricardo Lewandoski. 06 de abril de 2010.

[30] BRASIL. Supremo Tribunal Federal. **Súmula Vinculante n. 3.** 6 de jul de 2007.

[31] LX - a lei só poderá restringir a publicidade dos atos processuais quando a defesa da intimidade ou o interesse social o exigirem

das decisões judiciais, tanto pelas partes, quanto pela sociedade. Ele precisa ser visto com temperamentos, e relativizado em razão da sua colisão com diversos outros princípios ou direitos[32].

Ainda, é de se destacar que a publicidade é a regra, e o sigilo, a exceção, conforme dispõe o art. 5º, XXXIII[33], da Constituição Federal. Com isso, no Estado Democrático de Direito, a publicidade só deve ser inaplicada em razão do sigilo, o qual deve ser observado quando for imprescindível à segurança da sociedade e do Estado.

Nesse contexto, é de se ressaltar o princípio da motivação das decisões, estabelecido no art. 93, IX, da CF, supramencionado, o qual impõe a necessidade de motivação das decisões (judiciais e administrativas), bem como, que as sessões sejam públicas.

De fato, é possível constatar que uma decisão sem motivação corresponde a um verdadeiro óbice para o exercício do contraditório e ampla defesa pela parte que se sentir prejudicada, o que, consequentemente, viola o princípio do devido processo legal.

Em relação ao princípio da proibição de produção de provas ilícitas (art. 5º, LVI,), por vezes correlato ao princípio da motivação, é necessário destacar que com base na Teoria dos Frutos da Árvore Envenenada (*Fruits Of The Poisonous Tree*) e na CF, a prova obtida por meios ilícitos deve ser repudiada sempre pelos juízes e Tribunais, “por mais relevantes que sejam os fatos por ela apurados, uma vez que se subsume ela ao conceito de inconstitucionalidade [34] ". É nesse sentido o entendimento que vem sendo observado pelo STF. Destacamos, exemplificativamente, a seguinte ementa:

> HABEAS CORPUS" – INTERCEPTAÇÃO TELEFÔNICA – **NECESSIDADE DE A DECISÃO QUE A AUTORIZA POSSUIR FUNDAMENTAÇÃO JURIDICAMENTE**

---

[32] MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. Curso de direito constitucional. 6. ed. São Paulo: Saraiva, 2011. p. 448.

[33] XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado

[34] GRINOVER, Ada Pellegrini. Novas Tendências do Direito Processual. Rio de Janeiro: Forense, 1990, p. 62

> **IDÔNEA**, SOB PENA DE NULIDADE – IMPRESTABILIDADE DO ATO DECISÓRIO QUE, DESPROVIDO DE BASE EMPÍRICA IDÔNEA, RESUME-SE A FÓRMULAS ESTEREOTIPADAS CONSUBSTANCIADAS EM TEXTOS PADRONIZADOS REVESTIDOS DE CONTEÚDO GENÉRICO – **AUSÊNCIA DE EFICÁCIA PROBANTE DAS INFORMAÇÕES RESULTANTES DE PRORROGAÇÕES DE INTERCEPTAÇÃO TELEFÔNICA AUTORIZADAS POR DECISÃO DESTITUÍDA DE FUNDAMENTAÇÃO SUBSTANCIAL** – PRECEDENTES – A QUESTÃO DA ILICITUDE DA PROVA: TEMA IMPREGNADO DE ALTO RELEVO CONSTITUCIONAL – DIREITO FUNDAMENTAL DE QUALQUER PESSOA DE NÃO SER INVESTIGADA, ACUSADA, PROCESSADA OU CONDENADA COM BASE EM PROVAS ILÍCITAS (HC 93.050/RJ, REL. MIN. CELSO DE MELLO – RHC 90.376/RJ, REL. MIN. CELSO DE MELLO, v.g.) – **INADMISSIBILIDADE DA SUA PRODUÇÃO EM JUÍZO OU PERANTE QUALQUER INSTÂNCIA DE PODER – DISCUSSÃO EM TORNO DA ILICITUDE POR DERIVAÇÃO ("FRUITS OF THE POISONOUS TREE")** – DOUTRINA – PRECEDENTES – "HABEAS CORPUS" DEFERIDO – RECURSO DE AGRAVO IMPROVIDO. (grifos nossos) [35]

No que tange ao princípio do juiz natural, estatuído pelo art. 5º, incisos XXXVII e LIII, da CF, é de se inferir que o magistrado não deve ter interesse no litígio e que deve tratar as partes com igualdade[36].

É de se rememorar que na referida Convenção Americana de Direitos Humanos – da qual o Brasil é signatário –, o artigo 8º preceitua que todo indivíduo tem o direito de ser ouvido por um "juiz ou tribunal competente, independente e imparcial, estabelecido anteriormente pela lei". Citado princípio de fato decorre da garantia constitucional do devido processo legal. Nesse sentido, é a jurisprudência:

> (...) Tão antigo como antiga é a própria legislação – não há falar em jurisdição sem falar em juiz natural -, o princípio do juiz natural tem, ao fim e ao cabo, a finalidade de resguardar a legitimidade, a imparcialidade e a legalidade da jurisdição.[37]

---

[35] BRASIL. Supremo Tribunal Federal. **Agravo Regimental no *Habeas Corpus* 129.646.** Relator: Min. Celso de Mello. 03 de out de 2020.
[36] CUNHA JÚNIOR; NOVELINO, *op. cit*, p. 73.
[37] BRASIL. Superior Tribunal de Justiça. **Agravo Regimental no *Habeas Corpus* 106.590.** Relator: Min. Nilson Naves. 05 de maio de 2009.

O conteúdo do princípio do juiz natural se refere ao juízo adequado para o julgamento de determinada demanda, conforme as regras de fixação de competência e a proibição de juízos extraordinários ou tribunais de exceção (*ex post facto*), ou seja, constituídos após os fatos. Segundo entendimento doutrinário "o vocábulo 'natural' simboliza aquilo que é ordinário, que não é artificial, que pode ser reconhecido facilmente, que foi estabelecido sem qualquer tipo de manipulação, de forças que atuam externa ou internamente ao Judiciário."[38] .

A respeito do princípio da duração razoável do processo, estatuído no art. 5º, LXXVIII -incluído pela Emenda Constitucional n. 45/2004, necessário destacar que este tem o objetivo de assegurar a todos (no âmbito judicial e administrativo), a razoável duração do processo, e os meios que garantam celeridade na sua tramitação. Tal determinação também encontra respaldo no art. 8.1, da aludida Convenção Americana de Direitos Humanos (Pacto de São José da Costa Rica).

Todavia, relativamente ao princípio supra, é importante consignar também a dificuldade que temos para definir qual seria a "razoável duração do processo". A ementa abaixo retrata essa problemática:

> EMENTA AGRAVO REGIMENTAL NO HABEAS CORPUS. WRIT IMPETRADO ANTERIORMENTE NO SUPERIOR TRIBUNAL DE JUSTIÇA. DEMORA NO JULGAMENTO. VIOLAÇÃO DO PRINCÍPIO DA RAZOÁVEL DURAÇÃO DO PROCESSO. INCISO LXXVIII DO ARTIGO 5º DA CONSTITUIÇÃO FEDERAL. 1. **A sobrecarga de processos em trâmite nos Tribunais Superiores inviabiliza, na hipótese, compreender violada a garantia constitucional da razoável duração do processo, prevista no inciso LXXVIII do artigo 5º da Constituição Federal, em que distribuída a ação constitucional há pouco mais de um ano**. 2. Agravo regimental conhecido e não provido. (grifos nossos) [39]

Ademais, com um simples cotejamento dos demais princípios que vimos no que tange ao devido processo legal, é possível concluir que não necessariamente,

---

[38] RODRIGUES, Geisa de Assis. Anotações sobre o princípio constitucional do juiz natural. Constituição e Processo. In.: DIDIER JR., Fredie; WAMBIER, Luiz Rodrigues; GOMES JR., Luiz Manoel (org.). Salvador: JusPODIVM, 2007.

[39] BRASIL. Supremo Tribunal Federal. **Agravo Regimental no *Habeas Corpus* 119.451.** Relator: Min. Rosa Weber. 26 de nov de 2013.

um processo deve ser rápido. Ele precisa, de fato, durar tempo necessário e útil à solução da questão submetida ao órgão jurisdicional.

Em relação ao tratamento paritário conferido às partes do processo (princípio da igualdade processual), estabelecido pelo artigo 7º do CPC/2015, segundo lição de Fredie Didier[40], para a concretização desse princípio, é necessário observar a incidência das seguintes garantias:

> a) imparcialidade do juiz (equidistância em relação às partes); b) igualdade no acesso à justiça, sem discriminação (gênero, orientação sexual, raça, nacionalidade etc.); c) redução das desigualdades que dificultem o acesso à justiça, como a financeira (ex.: concessão do benefício da gratuidade da justiça, arts 98-102, CPC), a geográfica (ex.: possibilidade de sustentação oral por videoconferência, art. 937, §4º, CPC), a de comunicação (ex.: garantir a comunicação por meio da Língua Brasileira de Sinais, nos casos de partes e testemunhas com deficiência auditiva, art. 162, III, CPC) etc.; d) igualdade no acesso às informações necessárias ao exercício do contraditório.

Por fim, o processo, para ser devido, há de possuir outros atributos. Cada novo atributo corresponde a um princípio constitucional do processo, que, embora implícito, é de grande relevância. Daí surgem os princípios da adequação, da boa-fé processual e da efetividade, também decorrentes do devido processo legal[41].

Tais regras, constitucionalmente e legalmente estabelecidas, são destinadas a regular e limitar a atuação do Estado, visando o equilíbrio que a sociedade, por si só, não pode alcançar, bem como assegurar as liberdades dos cidadãos. Tem-se que o aludido princípio deve ser aplicado não apenas entre as partes do processo, mas por todos sujeitos, instituições e órgãos, públicos e privados, que exerçam, direta ou indiretamente, funções qualificadas como essenciais à justiça, de acordo com a Constituição[42].

---

[40] DIDIER, Fredie. Curso de Direito Processual Civil. Introdução ao Direito Processual Civil, Parte Geral e Processo de Conhecimento. Salvador: Ed. Juspodivm, 2019, p. 127.
[41] DIDIER JUNIOR, 2011, p. 49.
[42] MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. Curso de direito constitucional. 9. ed. rev. e atual. São Paulo: Saraiva, 2014, p. 485.

Ademais, conforme estudado no tópico anterior, com o advento das novas tecnologias, inúmeros são os desafios que emergem em decorrência da imperativa necessidade de a administração pública, em suposta conformidade com o princípio da eficiência (também disposto no artigo 37 da CF/88), adotar inovações tecnológicas de modo a, em tese, otimizar a entrega da prestação dos seus serviços. Todavia, é fundamental ter em mente que essas inovações devem aderir estritamente aos requisitos impostos pelo princípio do devido processo legal quando empregadas nos processos judiciais.

3. Contexto regulatório e deficiências existentes perante o devido processo legal

O Projeto VICTOR do Supremo Tribunal Federal foi o marco inicial para que outros tribunais brasileiros passassem a olhar para novas oportunidades.

Em 2019 foram identificados 47 projetos de inteligência artificial por Tribunais no país[43], o que demonstrou a necessidade de uniformização dos projetos para que problemas como falta da interoperabilidade, opacidade algorítmica, entre outros, acabassem por permear essa nova era da prestação jurisdicional.

Assim, em agosto de 2020 o Conselho nacional de Justiça elaborou a Resolução[44] n° 332, que cria regras para o desenvolvimento dessas tecnologias pelos Tribunais. O art. 2° estabelece os objetivos das IAs: "A Inteligência Artificial, no âmbito do Poder Judiciário, visa promover o bem-estar dos jurisdicionados e a prestação equitativa da jurisdição, bem como descobrir métodos e práticas que possibilitem a consecução desses objetivos".

O Capítulo II cita os direitos fundamentais presentes na Constituição Federal e Tratados que o país seja parte (art. 4°), sempre com a finalidade de busca da segurança jurídica e igualdade de tratamentos em casos iguais (art. 5º).

---

[43] SALOMÃO, Luiz Felipe. Tecnologia aplicada à gestão dos conflitos no âmbito do Poder Judiciário brasileiro. **Rio de Janeiro: Centro de Inovação, Administração e Pesquisa do Judiciário da Fundação Getúlio Vargas**, 2020.

[44] BRASIL. Conselho Nacional de Justiça. Resolução n° 332, de 21 de agosto de 2022. Dispõe sobre a sobre a ética, a transparência e a governança na produção e no uso de Inteligência Artificial no Poder Judiciário e dá outras providências. Disponível em: https://atos.cnj.jus.br/files/original191707202008255f4563b35f8e8.pdf . Acesso em 11 de set de 2023.

Também foram inseridos requisitos mínimos de transparência[45] para os sistemas (art. 8º) mas com claro foco de governança, e não para fácil compreensão e acesso de cidadãos. Chama atenção, em particular, o inciso VI, que trata sobre fornecimento de explicação quando a tecnologia apresentar proposta de decisão, mas sem indicar como essa explicação deverá ocorrer e se pode ser de fácil acesso a qualquer interessado/parte afetada.

Ainda, o Capítulo VII estabelece mecanismos para controle dos usuários, sendo dividido em usuários internos (art. 17) ou usuários externos (art. 18). Particularmente aos usuários externos, categoria em que estão os advogados e partes (art. 3º, inciso VI), existe previsão expressa acerca da necessidade de informação do uso de IAs indicando que o sistema somente auxilia a tomada de decisões, que é submetida à autoridade competente.

Dois pontos chamam atenção sobre a Resolução em questão: (i) inexiste citação expressa do respeito ao devido processo legal como um balizador do desenvolvimento dessas tecnologias, bem como (ii) também não há menção para que outros agentes interessados sejam consultados sobre a elaboração/implementação desses sistemas (tal como a Ordem dos Advogados do Brasil).

Em ralação ao primeiro ponto, é de se reconhecer, conforme identificado no item acima, que o princípio do devido processo legal tem várias dimensões normativas específicas que as inteligências artificiais, desde aquelas mais simples para busca textual, colocam em xeque. Por exemplo, citamos a imparcialidade do julgador, presente também em instrumentos internacionais que o Brasil é signatário, que pode ser violada pela utilização de algoritmos de busca jurisprudencial imbuída de um determinado viés e entrega somente decisões que privilegiam uma

[45] I – divulgação responsável, considerando a sensibilidade própria dos dados judiciais; II – indicação dos objetivos e resultados pretendidos pelo uso do modelo de Inteligência Artificial; III – documentação dos riscos identificados e indicação dos instrumentos de segurança da informação e controle para seu enfrentamento; IV – possibilidade de identificação do motivo em caso de dano causado pela ferramenta de Inteligência Artificial; V – apresentação dos mecanismos de auditoria e certificação de boas práticas; VI – fornecimento de explicação satisfatória e passível de auditoria por autoridade humana quanto a qualquer proposta de decisão apresentada pelo modelo de Inteligência Artificial, especialmente quando essa for de natureza judicial.

determinada interpretação, sem entregar o contexto de divergências que porventura possa existir em um determinado tema.

Ainda que a igualdade seja citada na regulamentação do CNJ, ela não deixa claro como medidas concretas devem ser adotadas para implementar o conteúdo normativo dessa dimensão no momento da decisão sobre a adoção dessas tecnologias.

Outra dimensão do princípio em análise que não está claramente regulamentada é a necessidade da motivação das decisões judiciais em casos que a inteligência artificial pode gerar um primeiro rascunho sobre o caso ou na substituição total do magistrado em casos pré-determinados. Esse problema já está em debate com algumas propostas concretas:

Reside nesse ponto alguns entraves à substituição ilimitada da figura do julgador por máquinas. O inciso exige uma expressa explicitação da relação do ato normativo com a causa ou a questão decidida. Casos concretos com muitas variáveis e disposições normativas envoltas de diversas causas de pedir próximas e remotas podem experimentar problemas de insuficiência de fundamentação por ocasião da massificação de decisões via IA. Por óbvio, isso não será problema para despachos repetitivos, decisões repetitivas, sentenças padrões, ou decisões monocráticas de relator, a exemplo, respectivamente, do despacho que determina a citação inicial em execução fiscal, da decisão que determina a penhora on-line de ativos financeiros, da sentença de extinção do processo por pagamento ou desistência ou da decisão monocrática de relator que julga prejudicado o agravo de instrumento face à sentença exarada pelo juiz de primeiro grau[46].

Ainda que a indicação de um rascunho de decisão possa ser comparada ao trabalho de um assessor (prática forense de todos os tribunais brasileiros) para decisões repetitivas que devem passar pelo crivo e assinatura de um magistrado, a diferença reside justamente no elemento da quantidade: dificilmente o magistrado irá analisar centenas ou milhares de rascunhos de decisões geradas pela tecnologias em poucos minutos, enquanto os assessores possuem um potencial limitado de produção e podem identificar problemas específicos que demandam análises

[46] SIQUEIRA, MORAIS e SANTOS, *op cit*, p. 16

aprofundadas sobre um caso que, inicialmente, poderia ser enquadrado como simples.

Ademais, a obrigação da motivação das decisões judiciais, aliada ao direito da ampla defesa, também pode sofrer violações pela opacidade dos algoritmos adotados, que podem não ser claros nos elementos que foram utilizados para chegar à decisão, levando à um questionamento da própria legitimidade de decisões formuladas por algoritmos. Esse problema não existe somente na hipótese da substituição total de julgadores, mas até quando a tecnologia é utilizada para uma primeira versão da decisão.

Alguns autores propõem uma sistematização de requisitos, empíricos e normativos, para que as decisões tomadas por algoritmos em processos judiciais sejam legítimas: transparência, consistência e comunicação efetiva[47].

Inteligências artificiais baseadas em modelos de aprendizado de máquina são de difícil transparência, uma vez que não permitem estabelecer o nexo causal entre a decisão e o conjunto de informações analisadas. Segundo Wingerden *et al:*

> Models based on machine learning are much less transparent, especially because it is not always or immediately clear why certain factors have a certain value for the sentencing decision. Machine learning looks for relations between characteristics that best predict the outcome. It does not look for characteristics that should affect the punishment according to legal principles. The transparency is limited to showing which factors predict the sentencing outcome, and this makes the sentencing decision unclear. Moreover, today's most effective machine learning uses the black box method: data come into the model and results come out—the process and method by which that happens are not the focus of the task[48].

---

[47] VAN WINGERDEN, S. G. C. et al. Artificial Intelligence and Sentencing: Humans against Machines. **Studies in Penal Theory and Philosophy**, p. 230-251, 2022.

[48] Os modelos baseados em aprendizagem automática são muito menos transparentes, especialmente porque nem sempre ou imediatamente é claro por que determinados fatores têm um determinado valor para a decisão da sentença. O aprendizado de máquina procura relações entre características que melhor preveem o resultado. Não busca características que devam afetar a punição segundo os princípios jurídicos. A transparência limita-se a mostrar quais os factores que predizem o resultado da sentença, o que torna a decisão da sentença pouco clara. Além disso, o aprendizado de máquina mais eficaz da atualidade usa o método da caixa preta: os dados entram no

Conforme a complexidade da tarefa desempenhada, não só há um impedimento no entendimento do processo realizado para chegar à uma determinada conclusão, mas até mesmo a impossibilidade de entendimento do porquê de determinado processo ser adotado, o que leva preocupações sobre os vários níveis de transparência necessários para a explicabilidade da decisão[49].

Outro elemento empírico que é apontado como necessário para a legitimidade de decisões judiciais é a consistência para com o ordenamento jurídico para garantir a segurança jurídica, ainda que seja um problema existente tanto para juízes humanos como para decisões tomadas por algoritmos[50].

Questões sobre vieses discriminatórios que permitem a reprodução de estigmas sociais, seja consequência da base de dados utilizada no treinamento ou dos vieses humanos dos programadores que elaboraram a estrutura técnica inicial são apontados como grandes desafios para esse requisito[51].

O último requisito apontado como necessário para a legitimidade é a comunicação efetiva sobre a decisão, principalmente acerca de como o processo decisório chegou à determinada conclusão e por que aquela foi tomada [52]. Diferentemente da transparência, esse requisito tem relação com a qualidade dos argumentos elencados nos atos decisórios e o poder de convencimento das partes por eles afetadas.

No caso de decisões tomadas por algoritmos, um dos problemas associados é a aversão das partes afetadas pelo algoritmo a aceitá-la como legitima, considerando a falta de capacidade de persuasão que os argumentos de uma máquina podem ter perante humanos:

> When considering machine judges' decisions and their ability to persuade the participants of the procedure or the public, the concept of algorithm aversion

---

modelo e os resultados saem – o processo e método pelo qual isso acontece não são o foco da tarefa (tradução nossa). *Ibidem*, p. 242

[49] A literatura técnica tenta criar vários tipos de taxonomias e sistemas para garantir a explicabilidade de deciões algorítmicas com modelos de aprendizado de máquina e aprendizado profundo. Ver ARRIETA, Alejandro Barredo et al. Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. Information fusion, v. 58, p. 82-115, 2020.

[50] VAN WINGERDEN *et al*, *op. cit*, p. 243

[51] *Ibidem*, p. 244

[52] *Ibidem*, p. 235

> seems an important one to consider (Burton, Stein, and Jensen 2020; Dietvorst, Simmons, and Massey 2015). Algorithmic aversion is a bias that causes humans to mistrust algorithmic decisions simply because they are not human—despite AI's record of sounder decisions. When considering AIbased decisions, the margin of error humans are willing to tolerate is none.[53]

A visão dos três elementos para a legitimidade de decisões judiciais por inteligência artificial, principalmente a transparência algorítmica, já são abordados na Resolução 332/2022 do CNJ em vários pontos: requisitos para a publicidade (art. 8), obrigações sobre governança (art. 9°), necessidade de explicabilidade das decisões (art. 19), entre outros.

Ocorre que a citada resolução não indica parâmetros claros e requisitos procedimentais que garantam esses critérios, ficando aberto aos agentes envolvidos no desenvolvimento (identificado somente como usuário interno pelo art. 3º, inciso V da Resolução, e limitado à membro, servidor ou colaborador do Poder Judiciário) o entendimento sobre o cumprimento desses requisitos.

Esse problema está diretamente conectado ao segundo problema já apontado no início do presente item do trabalho: que não existe previsão da participação de agentes de fora do Poder Judiciário no desenvolvimento dos sistemas, tal como representantes da Ordem dos Advogados do Brasil. Pode-se falar que há uma espécie de viés dos algoritmos desenvolvidos sob o atual formato para que eles realizem as atividades no melhor interesse dos servidores, tal como a celeridade no julgamento de processos, e não no melhor interesse da sociedade como parte afetada pelas decisões.

As consequências desse modelo já começam a aparecer como elemento de irresignação em alguns processos judiciais. No julgamento do RE nos EDcl no

---

[53] Ao considerar as decisões dos juízes automáticos e sua capacidade de persuadir para os participantes do procedimento ou para o público, o conceito de aversão ao algoritmo parece importante a considerar (Burton, Stein e Jensen 2020; Dietvorst, Simmons e Massey 2015). A aversão algorítmica é um viés que faz com que os humanos desconfiem das decisões algorítmicas simplesmente porque elas não são humano – apesar do histórico de decisões mais sólidas da IA. Ao considerar decisões baseadas em IA, a margem de erro que os humanos estão dispostos a tolerar é nenhuma (tradução nossa). *Ibidem*, p. 245

REsp 1945051 de Relatoria do Ministro Jorge Mussi, por exemplo, a parte Recorrente consignou expressamente:

> "(...) alega que teria fundamentado suficientemente o apelo nobre. Assevera que o entendimento desta Corte Superior, **supostamente confeccionado por intermédio de inteligência artificial (IA)**, seria nulo, porquanto "o acórdão recorrido destoa dos padrões jurisprudenciais sobre a admissibilidade do recurso especial, vazados no prequestionamento implícito e que nunca se exigiu oposição de embargos de declaração quando presente aquela forma de prequestionamento aceita, ou mesmo para discutir a nulidade dos acórdãos dos tribunais de segundo grau " (e-STJ fl. 544). (...) Argumenta que a "impossibilidade de saber as razões **pelas quais a máquina ofereceu a decisão e quais foram os parâmetros do algoritmo para a resposta se mostra disruptiva dos valores do Estado Democrático de Direito**, do devido processo legal e do dever de fundamentação, pois não se pode tomar decisões a partir de caixa preta, já que um pressuposto da democracia é que os cidadãos e cidadãs tenham ciência dos critérios das decisões" (e-STJ fl. 546). (...) Pondera que **"acórdão se trata de decisão 'pré-fabricada', 'genérica' e que se produziu por meio da máquina ou da ferramenta de 'copiar, colar' , sem qualquer tipo de vinculação com a causa ou com os textos do acórdão de origem e do Recurso Especial"** (e-STJ fl. 548). Destaca que "se constata a dissociação semântica do acórdão com o texto e contexto do Especial. Não pertinência, nem tampouco coerência entre os pedidos, causas de pedir e o que consta no acórdão recorrido. A máquina produziu uma resposta dissonante de todo o caso, vez que o texto que consta não se adequa à pretensão recursal, enquanto outros temas da pretensão recursal não foram sequer decididos" (e-STJ fl. 548). Acrescenta que "o texto do acórdão é fruto do viés da jurisprudência defensiva, sem conexão alguma acerca das matérias discutidas na Instância do STJ, de acordo com os contornos das pretensões recursais entabuladas, afigura-se que os obstáculos insubsistentes ou inexistentes, apenas se tratando de criação pelo algoritmo" (e-STJ fl. 549). Aduz que teria realizado o prequestionamento implícito da matéria infraconstitucional e faria jus a ver julgado o mérito do recurso especial, notadamente porque "não se colhe nenhum texto proibitivo ou restritivo quanto à admissibilidade do recurso, a partir de que a pretensão de nulidade do acórdão

> recorrido tenha que ser precedida de Embargos de Declaração opostos na origem" (e-STJ fl. 550). Postula, por derradeiro, "**a necessidade da conversão do julgamento em diligências para averiguação do tratamento do processo, seus dados e informações pelos sistemas artificiais, e sobre se a decisão agravada foi tomada com apoio na máquina ou pela máquina, mostra-se alicerçada no direito de o Recorrente se opor ao tratamento realizado (art. 18, § 2º, da LGPD) e de solicitar revisão da decisão, a partir do acesso aos critérios das operações realizadas no tratamento (art. 20, caput e § 1º, da LGPD)" (e-STJ fl. 561).** Requer, ao final, a admissão do recurso e sua remessa ao Supremo Tribunal Federal. [54] (grifos nossos)

Em outro caso, RE nos AREsp 2158875, de relatoria do Ministro Herman Benjamin também é possível verificar o descontentamento da parte com o uso de IA. Senão vejamos o seguinte trecho do seu recurso:

> "(...) O recorrente alega a existência de Repercussão Geral, bem como violação ao art. 93, IX, da CF/1988. Afirma que a decisão monocrática da Presidência do Tribunal, ao **não admitir os Embargos de Divergência com uso de inteligência artificial**, ofendeu o citado dispositivo constitucional, tendo reproduzido argumentos que se prestariam a fundamentar qualquer outro tipo de decisão. Afirma, ainda, que o acórdão da Corte Especial que confirmou referida decisão monocrática também padece do mesmo vício, não tendo enfrentado o fundamento da (in)aplicabilidade, ao caso, da Súmula 315/STJ. Requereu a admissão e o provimento do recurso (fls. 1.292-1.310, e-STJ).[55]

Todavia, em ambos os casos, tais argumentos foram afastados pela existência de óbices processuais para o processamento dos pedidos (ausência de comprovação do requisito de existência de repercussão geral) o que acarretou a negativa de seguimento de ambos os pleitos. Ou seja, as questões supra destacadas sequer foram decididas, demonstrando que inúmeros requisitos constitucionais

---

[54] BRASIL. Superior Tribunal de Justiça. **Recurso Extraordinário nos Embargos de Declaração no Agravo Interno do Recurso Especial n° 1945051.** Relator: Min. Jorge Mussi. 12 de maio de 2023.
[55] BRASIL. Superior Tribunal de Justiça. **Recurso Extraordinário no Agravo Regimental nos Embargos de Divergência em Agravo em Recurso Especial n° 2158875.** Relator: Min. Herman Benjamin. 07 de agosto de 2023.

podem ser renegados às partes pela adoção de novas tecnologias com o único e exclusivo objetivo de maior celeridade de julgamentos e diminuição de acervos.

Resta claro que, sob o atual regime da Resolução 322 de 2020 do CNJ, a adoção de inteligência artificial pelo Poder Judiciário no Brasil pode gerar mais violações à direitos do que gerar bem-estar social.

Conclusão

O Brasil atualmente passa por um momento de revolução digital no Judiciário com a substituição de processos e procedimentos por algoritmos que podem realizar tarefas complexas em questão de segundos.

O presente texto demonstrou que o arcabouço regulatório é insuficiente para garantir que direitos fundamentais e o bem-estar social sejam sacrificados em prol da celeridade.

No primeiro item foi estudado quais os tipos de tecnologias estão sendo desenvolvidos na área jurídica e as principais utilizações para o Poder Judiciário.

O segundo capítulo dedicou-se especificamente à abordagem da questão do Devido Processo Legal, um dos pilares inabaláveis do Estado Democrático de Direito, e a sua interação com as IAs. Nele, foi realizado uma análise doutrinária aprofundada e analisada a atual da jurisprudência da questão objeto do presente estudo e da legislação relacionada a esse princípio fundamental.

O terceiro capítulo realizou uma análise da Resolução n° 332 de 2022 do Conselho Nacional de Justiça e a insuficiência das disposições para garantir todas as garantias que decorrem do princípio do Devido Processo Legal para os jurisdicionados.

REFERÊNCIAS

ALBUQUERQUE, Adriana. PODER ARTIFICIAL DE TRIBUTAR – LIMITES E REQUISITOS À UTILIZAÇÃO (ADEQUADA) DA INTELIGÊNCIA ARTIFICIAL PELA ADMINISTRAÇÃO TRIBUTÁRIA. Londrina: Toth, 2023.

ARRIETA, Alejandro Barredo et al. Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. Information fusion, v. 58, p. 82-115, 2020.

BARACHO, José Alfredo Oliveira. Processo Constitucional. In: ____. Direito processual constitucional: aspectos contemporâneos. [s.n.t.]

BRASIL. Conselho Nacional de Justiça. Resolução n° 332, de 21 de agosto de 2022. Dispõe sobre a sobre a ética, a transparência e a governança na produção e no uso de Inteligência Artificial no Poder Judiciário e dá outras providências. Disponível em: https://atos.cnj.jus.br/files/original191707202008255f4563b35f8e8.pdf . Acesso em 11 de set de 2023.

BRASIL. Superior Tribunal de Justiça. **Agravo Regimental no *Habeas Corpus* 106.590.** Relator: Min. Nilson Naves. 05 de maio de 2009. Disponível em: https://processo.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=200801070259&dt_publicacao=01/06/2009 . Acesso em 30 de set de 2023.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nos Embargos de Declaração no Agravo Interno do Recurso Especial n° 1945051.** Relator: Min. Jorge Mussi. 12 de maio de 2023. Disponível em: https://processo.stj.jus.br/processo/dj/documento/mediado/?tipo_documento=documento&componente=MON&sequencial=153249157&num_registro=202101906468&data=20220513 . Acesso em 30 de set de 2023.

BRASIL. Superior Tribunal de Justiça. **Recurso Extraordinário no Agravo Regimental nos Embargos de Divergência em Agravo em Recurso Especial n° 2158875.** Relator: Min. Herman Benjamin. 07 de agosto de 2023. Disponível em https://processo.stj.jus.br/processo/dj/documento/?&sequencial=198336480&num_registro=202202003808&data=20230807&data_pesquisa=20230807&componente=MON . Acesso em 30 de set de 2023.

BRASIL. Supremo Tribunal Federal. **Agravo Regimental no *Habeas Corpus* 129.646.** Relator: Min. Celso de Mello. 03 de out de 2020. Disponível em https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754031215 . Acesso em 30 de set de 2023.

BRASIL. Supremo Tribunal Federal. **Agravo Regimental no *Habeas Corpus* 119.451.** Relator: Min. Rosa Weber. 26 de nov de 2013. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=5010105 . Acesso em 30 de set de 2023.

BRASIL. Supremo Tribunal Federal. **Agravo Regimental no Recurso Extraordinário 594.040.** Relator: Min. Ricardo Lewandoski. 06 de abril de 2010. Disponível em https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=610248 . Acesso em 30 de set de 2023.

BRASIL. Supremo Tribunal Federal. **Súmula Vinculante n. 3.** 6 de jul de 2007. Disponível em: https://jurisprudencia.stf.jus.br/pages/search/seq-sumula739/false . Acesso em 27 de set de 2023.

CONVENÇÃO Americana de Direitos Humanos. 22 de nov de 1969. Disponível em: https://www.pge.sp.gov.br/centrodeestudos/bibliotecavirtual/instrumentos/sanjose.htm . Acesso em 27 de set de 2023

CUNHA JÚNIOR, Dirley da; NOVELINO, Marcelo. **Constituição Federal para concursos**. 2. ed. rev., ampl. e atual. Salvador: Juspodivm, 2011. p. 93.

DIDIER JUNIOR, Fredie. Curso de direito processual civil: introdução ao direito processual civil e processo de conhecimento. 13. ed. Salvador: Juspodivm, 2011. v. 1, p. 45.

DIDIER, Fredie. Curso de Direito Processual Civil. Introdução ao Direito Processual Civil, Parte Geral e Processo de Conhecimento. Salvador: Ed. Juspodivm, 2019.

DINAMARCO, Cândido Rangel. Instituições de Direito Processual Civil. 7 ed. São Paulo: Malheiros Editores, 2015, v. 1, p. 250.

FUX, Luiz. Curso de Direito Processual Civil. 5ª Edição. Rio de Janeiro: Forense, 2022.

GRINOVER, Ada Pellegrini. Novas Tendências do Direito Processual. Rio de Janeiro: Forense, 1990.

JUNQUILHO, Tainá Aguiar. Inteligência Artificial no Direito – Limites Éticos. São Paulo: Juspodivm, 2022.

STRECK, Lenio Luiz. Dicionário de hermenêutica: 50 verbetes fundamentais da teoria do direito à luz da crítica hermenêutica do direito. 2. ed. Belo Horizonte: Casa do Direito, 2020.

LIU, Han-Wei; LIN, Ching-Fu; CHEN, Yu-Jie. Beyond State v Loomis: artificial intelligence, government algorithmization and accountability. **International journal of law and information technology**, v. 27, n. 2, p. 122-141, 2019.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. Curso de direito constitucional. 9. ed. rev. e atual. São Paulo: Saraiva, 2014.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. Curso de direito constitucional. 6. ed. São Paulo: Saraiva, 2011.

RODRIGUES, Geisa de Assis. Anotações sobre o princípio constitucional do juiz natural. Constituição e Processo. In.: DIDIER JR., Fredie; WAMBIER, Luiz Rodrigues; GOMES JR., Luiz Manoel (org.). Salvador: JusPODIVM, 2007.

SALOMÃO, Luiz Felipe. Tecnologia aplicada à gestão dos conflitos no âmbito do Poder Judiciário brasileiro. **Rio de Janeiro: Centro de Inovação, Administração e Pesquisa do Judiciário da Fundação Getúlio Vargas**, 2020.

SALOMÃO, Luiz Felipe. Tecnologia aplicada à gestão dos conflitos no âmbito do Poder Judiciário brasileiro. **Rio de Janeiro: Centro de Inovação, Administração e Pesquisa do Judiciário da Fundação Getúlio Vargas**, 2020.

SILVA, José Afonso da. **Curso de direito constitucional positivo**. 25. ed. rev. e atual. São Paulo: Malheiros, 2005.

SIQUEIRA, Dirceu Pereira; MORAIS, Fausto Santos de; SANTOS, Marcel Ferreira dos. Inteligência artificial e jurisdição: dever analítico de fundamentação e os limites da substituição dos humanos por algoritmos no campo da tomada de decisão judicial. **Sequência (Florianópolis)**, v. 43, p. e90662, 2023.

SOURDIN, Tania. Judge v Robot?: Artificial intelligence and judicial decision-making. **University of New South Wales Law Journal, The**, v. 41, n. 4, p. 1114-1133, 2018.

VAN WINGERDEN, S. G. C. et al. Artificial Intelligence and Sentencing: Humans against Machines. **Studies in Penal Theory and Philosophy**, p. 230-251, 2022.

2. O CONTEXTO BRASILEIRO DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

 https://doi.org/10.36592/9786554600798-02

Cacyone Gomes Barbosa Gonçalves Lavareda[1]

RESUMO
Este estudo tem como objetivo analisar o reconhecimento e consolidação do Direito Fundamental à Proteção de Dados Pessoais no contexto jurídico brasileiro. Por meio de uma abordagem histórica, hermenêutica e jurídica, explorou-se a trajetória desse direito desde seu surgimento na sociedade da informação até sua inserção na Constituição Federal por meio da Emenda Constitucional 115/2022. A metodologia adotada foi a análise documental, utilizando legislações pertinentes, decisões judiciais e contribuições doutrinárias. A evolução observada reflete a crescente importância da proteção de dados no contexto tecnológico, enfatizando a necessidade de interpretações precisas para fortalecer a proteção dos titulares de dados e garantir um ambiente digital seguro e ético.
Palavras-chave: Proteção de Dados, Direito Fundamental, Sociedade da Informação, Privacidade.

1. INTRODUÇÃO

No cenário contemporâneo, marcado pela acelerada evolução tecnológica e pela digitalização abrangente, surge uma preocupação que transcende fronteiras e impacta a vida de bilhões de indivíduos em todo o mundo: a proteção de dados pessoais. Os avanços tecnológicos revolucionaram a forma como informações pessoais são coletadas, armazenadas e compartilhadas, desafiando a privacidade e a segurança das pessoas. Nesse contexto, a Lei Geral de Proteção de Dados

---

[1] Professora de Direito Digital e Proteção de Dados Pessoais, palestrante, advogada e jornalista. Mestre em Direito Constitucional pelo IDP (Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa); Data Protection Officer (DPO) pelo European Centre of Privacy and Cibersecurity (ECPC), Universidade de Maastricht (Holanda). Mestranda em Direito Civil na Faculdade de Direito do Recife (UFPE). Especialista em Direito Digital LLM Universidade Católica de Pernambuco (UNICAP). Pós graduada em direito digital pela UNIDOMBOSCO. Pós-graduada em LGPD e GDPR pela Fundação Escola Superior do Ministério Público (FMP). DPO pela Academy of European Law (ERA-Germany). DPO pelo Instituto de Pesquisas Sociais, políticas e econômicas (IPESPE). Pesquisadora CEDIS / IDP PRIVACY LAB. Certificada pela IAPP / CIPM. Certificações pela L'université Paris Panthéon-Sorbonne, pela Dataprivacy Brasil, Exin, ABNT normas NBR ISO/IEC 27017 e 27018. Secretária da comissão de Proteção de Dados OAB/PE. Membro da Comissão Especial de Proteção de Dados do CFOAB.

Pessoais (LGPD) no Brasil e a legislação equivalente em diversas nações representam uma resposta necessária para salvaguardar os direitos fundamentais em um ambiente digital em constante transformação.

A LGPD, Lei nº 13.709/2018, é uma peça legislativa fundamental para regular o tratamento de dados pessoais em território brasileiro. Seu surgimento e implementação têm uma história intrincada, moldada por fatores como pressões da sociedade civil, demandas das empresas, desafios tecnológicos e até mesmo a crise global de saúde desencadeada pela pandemia da COVID-19. Através desta lei, o Brasil se alinhou a um movimento global em prol da proteção da privacidade e do controle dos cidadãos sobre seus próprios dados.

A vigência da LGPD, inicialmente prevista para agosto de 2020, enfrentou obstáculos e debates no Congresso Nacional, refletindo interesses diversos de setores econômicos e preocupações com a capacidade de conformidade das empresas. No entanto, a pandemia da COVID-19 lançou luz sobre a urgência de sua implementação, à medida que o uso indiscriminado de dados pessoais em nome da saúde pública se tornou uma realidade preocupante. O rastreamento de contatos, a geolocalização e o monitoramento de pacientes se tornaram ferramentas vitais no combate à pandemia, mas também desencadearam questões éticas e legais sobre privacidade e direitos individuais.

Neste contexto, a promulgação da LGPD e sua entrada em vigor trouxeram um novo conjunto de desafios e oportunidades. O tratamento responsável de dados pessoais agora é uma obrigação legal para empresas e organizações em todo o Brasil. Além disso, o reconhecimento pelo Supremo Tribunal Federal (STF) de que a proteção de dados é um direito fundamental autônomo reforçou sua importância e alcance na sociedade brasileira.

Este artigo explora a trajetória da LGPD, desde sua aprovação até sua implementação e suas implicações na sociedade. Será analisado como a pandemia da COVID-19 influenciou a urgência de regulamentação, assim como o papel do STF no reconhecimento desse novo direito fundamental. Também será possível compreender a relevância da LGPD para a proteção da privacidade e da liberdade dos cidadãos em um mundo cada vez mais interconectado.

2. O CONTEXTO BRASILEIRO DA LGPD

Para entender como foi criada a atual Lei Geral de Proteção de Dados Pessoais no Brasil (Lei nº 13.709/2018 ou LGPD) é necessário compreender seus antecedentes, a elaboração, e o contexto histórico somados aos quase dez anos de debates no executivo e no legislativo, nas universidades e na sociedade civil. Assim como fizemos com o GDPR.

A trajetória da Lei Geral de Proteção de Dados Pessoais no Brasil é permeada por discussões, polêmicas e comemorada pelos defensores dos consumidores. O projeto de lei de Proteção de Dados Pessoais (PL 53/2018) foi aprovado por unanimidade no Congresso Nacional depois de muita pressão da sociedade, e vista como uma vitória da democracia e como importante instrumento de defesa de milhões de pessoas, sobretudo do ponto de vista dos consumidores. Estes, especialmente, vítimas da perfilização e consequente discriminação. A aprovação da lei é o resultado de um longo trabalho feito por amplos setores da sociedade. Foram mais de nove anos de debate, duas consultas públicas, onze audiências públicas realizadas somente na comissão especial da Câmara e oito meses da campanha "Seus dados são você", da coalizão direitos na rede. [2] Contudo, rejeitada desde sempre pelo empresariado.

Em 2016, a Confederação Nacional da Indústria -CNI - através do Portal da Indústria sentiu ameaças ao setor, pois a Lei Geral de Proteção de Dados Pessoais não poderia impedir a inovação "o excesso de proteção das informações pessoais por meio da privacidade pode levar a efeitos indesejados, como a criação de obstáculos ao desenvolvimento econômico e tecnológico, à livre iniciativa e à livre concorrência".

Finalmente foi a Lei Geral de Proteção de Dados Pessoais sancionada em 14 de agosto de 2018 e mesmo assim, ainda neste mesmo ano, após sua sanção, a *Mobile Marketing Association* (MMA) considerou a Lei um empecilho que poderia causar prejuízos e desestimular a inovação. Pois ao fixar as mesmas exigências para

---

[2] IDEC,2018. **Após pressão da sociedade, Senado aprova Lei de Dados Pessoais**. Disponível em: https://idec.org.br/noticia/apos-pressao-da-sociedade-senado-aprova-lei-de-dados-pessoais. Acesso em: 10 nov. 2020.

companhias de diferentes portes, a lei elevaria o nível de exigência (técnica, de segurança e procedimental) a uma altura que startups e empresas menores dificilmente conseguiriam alcançar. Para o mercado, na lógica econômica e do lucro, corria-se o risco de desestimular a inovação e prejudicar o desenvolvimento da economia digital.[3]

Pois bem, voltando aos antecedentes da Lei Geral de Proteção de Dados Pessoais, quando surgiram os primeiros clamores de um novo direito que emergia diante da inovação, da tecnologia e já tinha reflexos na vida do cidadão titular de dados pessoais, na garantia da democracia, da liberdade de expressão e na economia, ressalta-se que a ausência de um quadro normativo específico não implicava, em absoluto, que a matéria não fosse relevante. Pois diversas situações relacionadas ao uso de dados pessoais geravam efeitos jurídicos que, por vezes, chegavam aos tribunais. No Brasil, portanto, e como não poderia ser diferente, os problemas relacionados ao tratamento de dados pessoais surgiram e foram, em boa parte, encaminhados, a despeito da existência de uma legislação geral a respeito[4]. A demanda crescente relacionada à utilização de dados pessoais não satisfazia a contento o problema em causa indo parar nas instâncias superiores já que não havia um regramento geral sobre o tema proteção de dados.

Para Doneda[5], nem a tão invocada formação da proteção da privacidade, como um dos direitos da personalidade até sua consolidação no artigo 5, incisos X e XII, com menção no Código Civil, artigo 21, foi capaz de proteger os indivíduos diante das novas tecnologias e suas questões. Dessa forma o perigo da demora em se reconhecer esse novo direito foi tamanho, pois ele ameaçava a sobrevivência de garantias preexistentes. Sua ausência também se traduzia em afronta ao Estado-Nação. A notícia do portal Nic.br, que faz parte do Comitê Gestor da Internet no Brasil, denunciou que robôs influenciaram eleições no Brasil, inclusive manipulando

---

[3] MMA, 2022. Sobre o MMA. 2022. Disponível em: **https://www.mmaglobal.com/files/documents/copia_de_mma-playbook-privacy_2018_pt-3.pdf**. Acesso em: 10 nov. 2020.

[4] DONEDA, Danilo; MENDES, Laura Shertel. **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021, p. 246.

[5] Idem.

algoritmicamente pessoas reais formando e utilizando-se dos seus perfis pessoais *on line*:

> Engana-se quem pensa que isso é coisa de eleição americana e treta EUA x russos. Se você é um desses, uma notícia desagradável: Somos influenciados pelos *bots* há pelo menos 2 eleições e até então ainda não havíamos nos dados conta. Quem garante isso é Dan Aranudo, professor brasileiro e pesquisador da Universidade de Washington, autor de um estudo que analisou como a propaganda computacional pode assumir a forma de contas automatizadas (*bots*), disseminar informações, manipular algoritmicamente pessoas reais e disseminar notícias falsas para moldar a opinião pública e influenciar na escolha de representantes.[6]

Ou seja, desde pelo menos 2006 já se havia dado conta do tamanho do perigo pela falta de uma regulação geral da proteção de dados pessoais no Brasil que ia na contramão de mais140 países onde essa garantia já era uma realidade há muitos anos.[7] Em alguns desses países, há pelo menos cinco, seis décadas, como já referenciado o caso da Alemanha no capítulo exordial. Mas, mesmo assim, o direito à proteção de dados pessoais percorreu um longo caminho legislativo a fim de garantir um mínimo legiferante até sua entrada em vigor em 18 setembro 2020 que ainda teve o risco de ser postergado por manobras parlamentares que pretendiam que a vigência da Lei Geral de Proteção de dados Pessoais fosse adiada. O que de fato ainda aconteceu com parte do seu texto, no que diz respeito à vigência das sanções e o ao estabelecimento do seu correspondente Órgão Administrativo Regulamentador, A Autoridade Nacional de Proteção de Dados (ANPD).

> A entrada em vigor da LGPD nesta sexta-feira (18) ocorreu devido à aprovação pelo Senado da MP 959/2020 (PLV 34/2020) no final de agosto. O texto original

---

[6] NIC.BR, 2018. Como robôs influenciaram as eleições de 2014 no Brasil. 2018. Disponível em: https://nic.br/noticia/na-midia/como-robos-influenciaram-as-eleicoes-de-2014-no-brasil/. Acesso em: 10 nov. 2020.

[7] GREENLEAF, G. Global Data Privacy Laws. 120 National Data Privacy Laws, Including Indonesia and Turkey. Privacy Laws & Business International. 2017. Disponível em: **https://ssrn.com/abstract=2993035**. Acesso em: 03 abr.de 2022.

> da medida previa o adiamento da vigência da LGPD para o fim do período de calamidade pública, conforme estabelecido no artigo 4º do PLV. Contudo, em atendimento à questão de ordem e a solicitações de lideranças partidárias, o presidente do Senado, Davi Alcolumbre, declarou a prejudicialidade desse dispositivo, que passou a ser considerado "não escrito" no projeto, transformado na Lei 14.058, de 2020. Davi lembrou que, em maio, o Senado aprovou destaque do PDT e do MDB que mantinha a vigência da LGPD para agosto de 2020. Não há previsão de nenhuma penalidade a empresas e pessoas quanto à entrada em vigor da LGPD. A Lei 14.010, de 2020 adiou de 1º de janeiro de 2021 para 1º de agosto de 2021 a vigência das sanções que a Autoridade Nacional de Proteção de Dados (ANPD), ainda pendente de instalação, pode aplicar nos órgãos, entidades e empresas que lidam com o tratamento de dados.[8]

Nessa análise de contextualização do nascimento da Lei Geral de Proteção de Dados é preciso também olhar para alguns dos principais acontecimentos e marcos com normas nacionais e internacionais (no caso, o Regulamento Geral Europeu de Proteção de Dados) que antecederam e influenciaram o novo diploma no Brasil. É possível elencar de maneira didática e robustamente contextualizada a trajetória da proteção de dados pessoais no Brasil, mesmo quando no dizer do próprio autor, existiam apenas centelhas que inspiraram uma sistemática própria. E essa retrospectiva é muito valiosa, pois desmistifica a ideia corrente de que o debate público brasileiro sobre o tema é recente, quando ele pode ser identificado desde 1970.[9]

No projeto, o Registro Nacional de Pessoas Naturais (RENAPE) seria um órgão de abrangência nacional, integrando o Registro Civil de Pessoas Naturais e a Identificação Civil e uma base de dados, que foi arquivado. Em 1978, também foi arquivado o projeto de Lei nº 4.365 de 1977, de autoria do deputado Faria Lima que criava um Registro Nacional de Bancos de Dados e normas de proteção da intimidade

---

[8] BRASIL, 2020. PL 4374 de 2020. Altera a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais, LGPD) e a Lei nº 12.414, de 9 de junho de 2011 para restringir o acesso, tratamento de compartilhamento de dados de consumidores por empresas de proteção ao crédito. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2261130 Acesso em: 3 set. 2022.

[9] DONEDA, 2021, Ibid., p. 247.

pelo uso indevido de dados arquivados em dispositivos eletrônicos de processamento de dados.[10]

Já em 1980, surgiu o projeto de Lei nº 2.796 de 1980, da Deputada Cristina Tavares que assegurava aos cidadãos acesso às suas informações constantes de bancos de dados e dava outras providências.[11] Apesar de arquivado, este projeto merece grande destaque, pois estava-se no caminho da luta pela redemocratização do país. A deputada Cristina Tavares deu corpo ao projeto que materializava princípios e direitos de cidadãos titulares de dados frente ao Estado no tratamento automatizado de dados pessoais e seu uso em bancos de dados públicos e privados, demonstrando aí as bases para a lei de proteção de dados. Embora não tivesse à época esse nome, era exatamente o que ela representava, um projeto de lei de proteção de dados pessoais extremamente bem contextualizado, justificado e aprovado com emendas sobretudo em relação ao seu parágrafo segundo que buscava garantir que as informações ali constantes fossem verídicas para evitar danos à personalidade.

> § 2.º Para efeito desta lei, considera-se tratamento automatizado de informações nominativas, todo o conjunto de operações realizadas pelos meios automáticos e que permitem, sob qualquer forma, a identificação das pessoas físicas às quais elas se aplicam.[12]

A justificativa do referido Projeto de Lei, em pleno ano de 1980, é um verdadeiro manifesto em defesa dos direitos da personalidade diante do uso dos dados pessoais dos indivíduos, que modificaria o artigo 9. do Código Civil e o art. 368 do Código Penal.

---

[10] BRASIL, 1977. Projeto de Lei 4.365 de 1977. Brasília: Diário do Congresso Nacional, 1977. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=FBF15270DD557906FEB1829EFEA68AED.proposicoesWeb1?codteor=1172300&filename=Avulso+-PL+2796/1980. Acesso em: 10 nov. 2020.

[11] BRASIL, 1980. Projeto de Lei 2.796 de 1980. Brasília: Diário do Congresso Nacional, 1980. Disponível em: https://imagem.camara.gov.br/Imagem/d/pdf/DCD23ABR1980.pdf#page=19. Acesso em: 10 nov. 2020.

[12] Idem.

Importa que a informática respeite quatro séries de valores dois tradicionais: os direitos do homem e as liberdades individuais ou públicas e dois mais propalados atualmente: a vida privada e a identidade humana.

A noção da vida privada aparece pela primeira vez na França na lei de 1970 que visa a reforçar a garantia dos direitos individuais, numa parte intitulada "proteção à vida privada". Essa lei modifica o art. 9. do Código Civil e o 368 do Código Penal a fim de aumentar a proteção à vida privada e à intimidade.

A noção de "identidade humana", primeiro objetivo citado pela nova lei. é o mais novo nos textos. A expressão é hoje utilizada em sociologia, em psicologia e nos estudos sobre a cultura e o saber.

Identidade se junta à personalidade sem, entretanto, se confundirem entre si. Refere-se ao que é essencial e singular em cada ser humano de acordo com seu tipo e seu meio. Em relação à informática, a palavra significa que a máquina deve respeitar o nome de cada um e não pode reduzir seus direitos à números anônimos.

A questão da privacidade é, sem dúvida, a mais polêmica das questões, a que mais publicidade tem recebido e a que produziu maiores consequências legais em diversos países.

A era do computador possibilitou, pelo menos potencialmente. a agregação de dados sobre indivíduos, dados esses antes dispersos em arquivos manuais. O "rastro que uma pessoa deixa hoje de sua passagem pode ser muito mais nítido e permanente com o uso. de computadores. Em consequência de extensões. debates públicos. alterações nas legislações vêm sendo propostas e tornadas efetivas, notadamente nos países adiantados.

A Suécia foi pioneira na alteração de sua legislação. Nos Estados Unidos, principalmente após Watergate e outras invasões da privacidade, houve grande impulso na legislação sobre a matéria.

Uma lei de 1975 regula os bancos de dados federais ou criados com ajuda federal. A lei contém dispositivos que possibilitam o conhecimento, por parte do público, dos bancos de dados existentes.

A Inglaterra também no final de 1975 publicou um estudo sobre a regulamentação de bancos de dados computadorizados. Textualmente diz que "a existência e objetivo de sistemas de informação devem ser publicamente

conhecidos, bem como a categoria de dados que manipulam, e é facultado o acesso aos mesmos, pelos interessados".

A lei canadense, que trata da proteção da vida privada, baseia-se no seguinte princípio: "os indivíduos têm direito à vida privada e ao acesso aos registros que contêm informações sobre sua pessoa, para todos os fins, mormente para assegurar que os mesmos sejam completos e as informações contidas exatas e compatíveis com o interesse público.

Lei da República Federal da Alemanha, datada de 27 de janeiro de 1977, em seu art. 4°, preceitua que qualquer pessoa tem acesso aos dados armazenados a seu respeito e pode corrigi-los quando não corresponderem à realidade.

Verifica-se pelas providências adotadas por vários países que o problema da proteção à privacidade do indivíduo é da maior atualidade, face ao impacto que a informação computadorizada causou no mundo moderno. Se por um lado, o desenvolvimento da informática possibilitou um grande avanço no sentido da imediata recuperação de dados, por outro, constitui ameaça à intimidade do cidadão.

Nada mais oportuno que, à semelhança de outros países, legislemos no sentido de salvaguardar o direito de cada um quanto ao sigilo e à retificação dos dados sobre sua pessoa.

Assim é que achamos por bem apresentar esta proposta e submetê-la ao arbítrio desta Casa, ciente de sua importância no resguardo dos princípios e direitos fundamentais do homem.

A Iniciativa não pretende ser a primeira e provavelmente não será a última, mas cremos que o momento é chegado de dar a nosso povo o direito de se precaver contra eventuais ofensas à sua integridade.

Submetemos, pois, à apreciação dos doutos pares este projeto de lei que, sem dúvida, sofrerá alterações de molde a aprimorá-lo no sentido de atender às justas reivindicações de todos quantos compreendem seu largo alcance.

Mas, após uma nova Comissão Especial destinada a dar parecer ao Projeto de Lei 364, do Poder Executivo, que dispunha sobre o Código Civil, requisitou esse e outros projetos de lei em tramitação. Em seguida a própria Cristina Tavares, em agosto de 1984, pediu desistência do Projeto de Lei e ele foi retirado de plenário e arquivado em 30 de maio de 1985, sem apresentação dos motivos no único

requerimento que consta dos autos do processo digital de tramitação (às folhas 40) do mesmo. O Habeas Data foi introduzido na Constituição Federal de 1988 em reação ao processo ditatorial no Brasil para que os cidadãos tivessem acesso às suas informações pessoais frente ao Estado e às injustiças que vinham sendo perpetradas durante aquele período:

> O habeas data foi introduzido, no Direito brasileiro, com a Constituição Federal de 1988. Conforme a definição constitucional, no inciso LXXII do art. 5o da Carta Magna, trata-se de um meio posto à disposição das pessoas para que conheçam as informações a seu respeito constantes de registros ou bancos de dados de entidades governamentais ou de caráter público, permitindo ainda que seja feita a retificação dos dados eventualmente inexatos.[13]

Dessa forma, mais que uma ação constitucional, o Habeas Data tem caráter de direito material quando garante aos cidadãos acesso às suas informações pessoais e o direito de corrigir retificando ou apagando o que eventualmente esteja incorreto ou por uma interpretação extensiva, o que consta incompleto.

Em 1984 no Rio de Janeiro, a Lei Estadual 824, de 28 de dezembro de 1984, que "Assegura o direito de obtenção de informações pessoais contidas em bancos de dados operando no Estado do Rio de Janeiro e dá outras providências"; e, em São Paulo, a Lei Estadual 5.702, de 5 de junho de 1987, que "Concede ao cidadão o direito de acesso às informações nominais sobre sua pessoa" que surgiram inspirados no projeto de lei anterior.

> Faço saber que a Assembleia Legislativa do Estado do Rio de Janeiro decreta e eu sanciono a seguinte Lei: Art. 1º - A toda pessoa física ou jurídica é assegurado, livre de qualquer ônus, o direito de conhecer as suas informações pessoais contidas em bancos de dados, públicos-estaduais e municipais - ou privados, operando no Estado do Rio de Janeiro, bem como de saber a procedência e o uso dessas informações e de completá-las ou corrigi-las, no caso de falhas ou inexatidões. Parágrafo único - Qualquer informação pessoal só poderá ser

---

[13] WALD, Arnoldo. O habeas data na Lei 9.507/97. In: WAMBIER, Teresa Arruda Alvim (Cood.). **Habeas data.** São Paulo: Revista dos Tribunais, 1998, p. 26.

> registrada com a identificação da fonte onde foi obtida. Art. 2º - Os bancos referidos no artigo anterior devem ter a existência divulgada, juntamente com sua finalidade, abrangência e categorias de informações arquivadas, bem como o nome do responsável pela sua administração. Art. 3º - O uso de informações pessoais para fins diversos daqueles para os quais foram obtidas depende do consentimento expresso da parte diretamente interessada, que poderá, ainda, contestar a relevância das informações a seu respeito para as finalidades declaradas do banco. Art. 4º - É vedada a transferência de dados pessoais de um banco de dados para outro cujas finalidades não sejam as mesmas, salvo prévio e expresso consentimento da pessoa envolvida. Art. 5º - Esta Lei entrará em vigor na data de sua publicação, revogadas as disposições em contrário.[14]

O que chama a atenção dessa Lei Estadual de 1984, é que seu conteúdo reflete quase na totalidade, o núcleo duro do Projeto de Lei 2.796 de 1980, da Deputada Cristina Tavares, que assegurava aos cidadãos acesso às suas informações constantes de bancos de dados e dava outras providências, tocando no assunto do compartilhamento de dados com finalidade diversa da coleta e a necessidade de consentimento expresso. Uma curiosidade, é que a Lei Estadual do Rio de Janeiro entra em vigor em dezembro de 1984, quatro meses depois que a Deputada Cristina Tavares pede desistência do Projeto de Lei nº 2.796 de 1980. Em 05 de junho de 1987, a Lei Estadual 5.702, no estado de São Paulo, concedendo ao cidadão o direito de acesso às informações nominais sobre sua pessoa.

No ano de 1988, na Constituição Federal, pela primeira vez, surge a garantia constitucional do *Habeas Data* em meio ao trauma dos brasileiros durante o período da ditadura. Um direito de buscar suas informações pessoais em relação ao Estado (órgãos públicos). "pode-se afirmar que o habeas data foi criado no Brasil durante a elaboração da Constituição de 1988, tendo sido inspirado na recente utilização, por autoridades públicas, de dados inteiramente falsos ou contendo erros, visando a fins políticos e com grave prejuízo de direitos individuais."[15]

---

[14] BRASIL, 1984. Lei nº 824, de 28 de dezembro de 1984. Assegura o direito de obtenção de informações pessoais contidas em bancos de dados operando no estado do rio de janeiro e dá outras providências. Brasília: 1984. Disponível em: **https://gov-rj.jusbrasil.com.br/legislacao/149858/lei-824-84.** Acesso em: 10 ago. 2022.

[15] DALLARI, Dalmo de Abreu. **Direitos Humanos e Cidadania.** São Paulo: Moderna. 2002.

Em 1988, também houve o estabelecimento da defesa do consumidor. Passa-se a receber as demandas relacionadas a dados pessoais e dois anos depois, em 1990, o Código de Defesa do Consumidor, que foi inspirado, de acordo com o responsável pela elaboração do anteprojeto, na normativa norte-americana de proteção ao crédito estabelecida pelo *National Consumer Act e pelo Fair Credt Reporting Act* – FCRA.[16]

Podendo-se nesta normativa observar princípios e extrair os direitos do consumidor sobre seus dados pessoais:

> SEÇÃO VI - Dos Bancos de Dados e Cadastros de Consumidores. Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. § 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos. § 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele. § 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas. § 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público. § 5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.[17]

No ano de 1991, a lei dos Arquivos Públicos (Lei 88.159/91) seria uma das primeiras leis ordinárias sobre proteção de dados. Ela consagra o direito do cidadão

[16] DONEDA, 2021, Ibid., p. 246.
[17] BRASIL, 1990. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em:
http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 10 ago. 2020.

de acesso à informação de seu interesse particular ou de interesse público, assim como a proteção do sigilo, da intimidade e da vida privada.

Em 2002, o Código Civil (Lei 10.406/2002), em seus artigos 12 e 21, considerando a proteção de dados pessoais como um dos aspectos da privacidade, e a privacidade sendo um direito da personalidade, esses artigos surgem como uma proteção da vida privada e de se fazer imediatamente cessar lesão à ameaça, e tendo entre as medidas, a responsabilidade de reparar perdas e danos causados. Já em 2003, conforme elencado por Doneda.[18] o Governo brasileiro assinou a Declaração de Santa Cruz de La Sierra reconhecendo ter consciência de que a proteção de dados pessoais é um direito fundamental:

> Estamos também conscientes de que a protecção de dados pessoais é um direito fundamental das pessoas e destacamos a importância das iniciativas reguladoras ibero-americanas para proteger a privacidade dos cidadãos, contidas na Declaração de Antigua, pela qual se cria a Rede Ibero-Americana de Protecção de Dados, aberta a todos os países da nossa Comunidade.[19]

Somente em 2004 foi promulgado o Acordo de *Santa Cruz de La Sierra* Constitutivo da Secretaria Geral Ibero-Americana, assinado pelo Brasil em 12 de julho de 2004, pelo decreto nº 6.659, de 20 de novembro de 2008, que determina em seu artigo 1º “O Acordo de Santa Cruz de La Sierra Constitutivo da Secretaria Geral Ibero-Americana, apenso por cópia ao presente Decreto, será executado e cumprido tão inteiramente como nele se contém”.[20] Apesar de o Governo brasileiro ratificar à época, que tinha consciência desse direito fundamental à proteção de dados pessoais, esse acordo, mesmo tendo conteúdo genérico não se evidenciou internamente nem tão pouco gerou repercussões para que se reconhecesse esse direito como fundamental por vários anos.

---

[18] DONEDA, Danilo. **Lei geral de proteção de dados (Lei n° 13.709/2018) a caminho da efetividade: contribuições para a implementação da LGPD**. São Paulo: Thomson Reuters, 2020, p. 250.

[19]DECLARAÇÃO de Santa Cruz de La Sierra documento final da XIII Cumbre Ibero-Americana de Chefes de Estado e de Governo, disponível em: **https://www.segib.org/wp-content/uploads/DECLARASAO-STA-CRUZ-SIERRA.pdf**. Acessado em março de 2021.

[20] BRASIL, 2008. Decreto n. 6659. Disponível em: **http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Decreto/D6659.**htm Acesso em: 14 de maio. 2021.

No ano de 2011 foi sancionada a Lei do Cadastro Positivo, lei nº 12.414, de 9 de junho de 2011. Que veio disciplinar a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito, apontada por Doneda[21], como a primeira norma brasileira que foi concebida a partir de conceitos e sistemática de proteção de dados já consolidada em outros países, mas frustrou a expectativa por não demonstrar de fato sua importância para cultura de formação de uma cultura jurídica de proteção de dados. De fato, como veremos posteriormente, essa lei não se demonstrou tão positiva assim aos olhos do consumidor e nem seu sistema de proteção. Também em 2011, foi sancionada a Lei de Acesso à informação (lei 12.527/2011) que de fato contribuiu para as bases da futura Lei Geral de Proteção de Dados.

> A Lei de Acesso à Informação (Lei 12.527/2011), que regulamenta o princípio constitucional da transparência, além de definir o que é informação pessoal de forma análoga à que posteriormente estaria presente na própria LGPD, possui, em seu artigo 31, um regramento específico para a proteção de dados pessoais em poder do poder público, pelo qual tais informações estariam disponíveis, a princípio, somente ao interessado até um período de cem anos de sua produção, salvo na verificação de algumas das exceções previstas no mesmo artigo.[22]

Embora depois de sancionada a Lei Geral de Proteção de Dados, esta passou a ser analisada por parte da doutrina como incompatível ou até divergente da Lei de Acesso à Informação, servindo inclusive para negar solicitações aos titulares dos dados o que tem causado embate entre as leis.[23]

O próprio caso da decretação do sigilo de cem anos dos filhos do presidente Jair Bolsonaro é exemplo disso, de acordo com Bruno Bioni, que defende que as leis são harmônicas entre si, o que acontece é um equívoco de interpretação. Nesse sentido, nota-se um padrão de violação das regras da Lei de Acesso à Informação

---

[21] DONEDA, 2020, Ibid., p. 251.
[22] DONEDA, 2020, Ibid., p. 251.
[23] BRASIL 2021. **Acesso à informação não pode ser prejudicado por conta de Lei de Proteção de Dados, dizem especialistas**. Agência Câmara de Notícias. Disponível em: https://www.camara.leg.br/noticias/828370-acesso-a-informacao-nao-pode-ser-prejudicado-por-conta-de-lei-de--protecao-de-dados-dizem-especialistas. Acesso em: 5 set. 2022.

relativas ao direito de acesso em razão do argumento de sigilo baseado na Lei Geral de Proteção de Dados, afastando do público informações de evidente interesse público. A má interpretação da Lei Geral de Proteção de Dados foi utilizada para embasar o sigilo de 100 anos, por exemplo, dos dados dos crachás de acesso dos filhos do presidente da república, Jair Bolsonaro, por serem dados pessoais; do cartão de vacinação do presidente e para não informar o salário do policial acusado de matar Marielle Franco, todos os casos embasados no fato de esses dados serem pessoais.[24]

Em 2012, mesmo insuficiente, podemos citar a Lei 12.737/12 (Lei Carolina Dickmann) sobre a invasão de dispositivos, comentada Tomasevicius Filho.[25] A atriz teve fotos íntimas obtidas de seu computador pessoal e divulgadas na Internet pelo fato de ela não se ter submetido à chantagem da pessoa que teve acesso a esse material. Tipificou-se o crime de interrupção ou perturbação de serviço telemático ou de informação de utilidade pública, como também o de "clonagem" de cartões de crédito e de débito, equiparando-se ao crime de falsificação de documento particular. Merece destaque a inserção do art. 154-A no Código Penal brasileiro, para estabelecer como crime a violação da privacidade por meio da invasão de dispositivo informático alheio:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

---

[24] BIONI, Bruno; SILVA, Paula; Pedro, Martins. **Intersecções e relações entre a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI)**: análise contextual pela lente do direito de acesso. Coletânea de artigos da pós-graduação em ouvidoria pública. 2022. Disponível em: https://revista.cgu.gov.br/Cadernos_CGU/article/view/504/284. Acesso em: 16 nov. 2022.

[25] TOMASEVICIUS FILHO, Eduardo. Em direção a um novo 1984? A tutela da vida privada entre a invasão de privacidade e a privacidade renunciada. R. Fac. Dir. Univ. São Paulo v. 109 p. 129 - 169 jan./dez. 2014. Disponível em: **https://www.revistas.usp.br/rfdusp/article/download/89230/96063/167402** Acesso em: 14 de maio. 2021.

Para Tomasevicius, essa lei foi meramente simbólica, porque as penas imputadas são muito brandas e não dissuadirão as pessoas que sentem compulsão a invasão de privacidade a deixarem de praticar essas condutas.[26]

Em 2014, o Marco Civil da Internet (Lei 12.965/2014) foi a legislação que mais se aproximou da Lei Geral de Proteção de Dados que estava por vir. Inclusive, na obra PROTEÇÃO DE DADOS CONTEXTO, NARRATIVAS E ELEMENTOS FUNDANTES, organizado por Bruno Bioni, até a plataforma criada para as discussões sobre o Marco Civil da Internet, foi utilizada para a primeira consulta pública sobre o Anteprojeto de Lei de Proteção de Dados.

> O processo de materialização desse interesse na criação de uma lei geral teve início na Secretaria de Assuntos Legislativos, em parceria com o Departamento de Proteção e Defesa do Consumidor, ambos do Ministério da Justiça, que, sob a coordenação de Laura Schertel Mendes e com a colaboração do então consultor Danilo Doneda, elaborou uma minuta de Anteprojeto de Lei de Proteção de Dados e, em dezembro de 2010, submeteu o texto a consulta pública, seguindo os moldes da elaboração da Lei n.º 12.975/2014 (Marco Civil da Internet).[27]

Por outro lado, o Marco Civil da Internet vinha numa necessidade crescente de proteção de dados pessoais posto que a lei foi sancionada pós revelações feitas por Edward Snowden sobre o esquema de vigilância em massa dos indivíduos através dos seus perfis pessoais, orquestrado pelo Governo Americano depois dos atentados das torres gêmeas, no histórico 11 de setembro. Francisco Brito Cruz descreve, conforme enxerto baixo, como o efeito "Snowden" influenciou diretamente o texto do Marco Civil da Internet quanto à privacidade e à proteção de dados.

> Por fim, o Projeto de Lei nº 2.126/2011 ganhou atenção especial quando o governo brasileiro tornou sua aprovação ponto de honra após o ex-funcionário da Agência Nacional de Segurança dos Estados Unidos da América, Edward Snowden, protagonizar um amplo vazamento de informações que abarcava, dentre outras denúncias, a espionagem da Petrobras e a interceptação do

[26] TOMASEVICIUS FILHO, 2021, Ibid.
[27] BIONI, 2022, Ibid., p. 19.

telefone pessoal da Presidenta Dilma Rousseff. De um lado ou de outro o tema do Marco Civil não passou batido no debate político, ao menos dentro de uma comunidade de usuários de Internet interessados no tema e de setores políticos, acadêmicos, econômicos e governamentais especializados.[28]

Nos anos de 2015, o parágrafo 6, acrescentado no Código de Defesa do Consumidor, pela Lei 13.146/2015 – Estatuto da Pessoa com Deficiência – passou a tratar de modo mais específico do acesso dos portadores de necessidades especiais. Da leitura desse artigo, a doutrina extrai: "i) o direito de acesso; ii) o princípio da qualidade dos dados; iii) o princípio da transparência; iv) o direito de retificação e cancelamento, e v) o princípio do esquecimento".[29]

No mesmo ano, o projeto de Lei nº 3.541/2015, entre outras medidas, propõe acrescentar os direitos básicos do consumidor: i) a privacidade e a segurança de informações e de seus dados pessoais coletados, inclusive, no meio eletrônico; e ii) a liberdade de escolha, vedados a discriminação e o assédio do consumo.[30]

Em 2016 foi aprovado em âmbito internacional aquela que seria a maior influência sobre a Lei Geral de Proteção de Dados Pessoais: o Regulamento Geral de Proteção de Dados Europeu. *"Em âmbito internacional, foi no intervalo de 2012 a 2016 que foi discutido e aprovado, em diferentes níveis, o Regulamento Geral de Proteção de Dados (RGPD) europeu, reconhecido como a maior influência da Lei Geral de Proteção de Dados"*.[31]

[28] CRUZ, Francisco Carvalho de Brito. **Direito, democracia e cultura digital**: A experiência de elaboração legislativa do Marco Civil da Internet. 138f. Dissertação (Mestrado em Direito) - Faculdade de Direito da Universidade de São Paulo. São Paulo, 2015. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2139/tde-08042016-154010/publico/dissertacao_Francisco_Carvalho_de_Brito_Cruz.pdf. Acesso em: 3 ago. 2022.

[29] DONEDA, 2021, Ibid. 246.

[30] BRASIL, 2015. O PL 3.514/2015 teve origem no PLS 281/2012, de autoria do Senador José Sarney PMDB/AP Disponível em: **www.camara.gov.br/proposicoesWeb/prop_mostrarintegra**. Acesso em: 3 ago. 2022.

[31] BIONI, Bruno; SILVA, Paula; Pedro, Martins. 2022, Ibid., p. 21.

Tabela 1 - Entenda O marco legal de proteção de dados

Estrutura	A Lei 13.709/18, tem 65 artigos, distribuídos em 10 Capítulos. O texto foi inspirado fortemente em linhas específicas da regulação europeia, o Regulamento Geral de Proteção de Dados (GDPR, em sua sigla em inglês)
Hipóteses para o tratamento de dados	Com o consentimento do titular; Para o cumprimento de obrigação legal ou regulatória pelo responsável pelo tratamento; Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas; Para a realização de estudos por órgão de pesquisa, sem a individualização da pessoa; Para a proteção da vida ou da incolumidade física do titular ou de terceiros; Para a tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; Para a execução de um contrato ou de procedimentos preliminares relacionados a um contrato do qual é parte o titular quando a seu pedido; Para pleitos em processos judicial, administrativo ou arbitral;
Abrangência	Quaisquer dados, como nome, endereço, e- mail, idade, estado civil e situação patrimonial, obtido em qualquer tipo de suporte (papel, eletrônico, informático, som e imagem, etc.).
Contratos de adesão	Nos casos de contratos de adesão, quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço, o titular deverá ser informado com destaque sobre isso.
Dados sensíveis	O texto traz o conceito de dados sensíveis, que recebem tratamento diferenciado: sobre origem racial ou étnica; convicções religiosas; opiniões políticas; filiação a sindicatos ou a organizações de caráter religioso, filosófico ou político; dados referentes à saúde ou à vida sexual; e dados genéticos ou biométricos vinculados a uma pessoa natural.
Sanções administrativas	Quem infringir a nova lei fica sujeito a advertência, multa simples, multadiária, suspensão parcial ou total defuncionamento, além de outras sanções.

Responsabilidade civil	O responsável que, em razão do exercício de atividade de tratamento de dados, causar a dano patrimonial, moral, individual ou coletivo, é obrigado a reparar. O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.

Fonte[32]

Depois de elencar as normas que influenciaram e estimularam a elaboração da Lei Geral de Proteção de Dados, é importante ressaltar que no Brasil, a referida lei, como já se percebe pelo exposto, percorreu um cenário de ameaças, resultando na sua lentidão. Foi um processo que se arrastou por mais de dez longos anos[33], deixando os brasileiros expostos às vulnerabilidades tecnológicas, ou melhor dizendo, vulnerabilidades digitais.

Para Doneda[34], os debates para uma futura Lei Geral de Proteção de Dados no Brasil, começaram ainda em 2005, no “I Seminário Internacional de Proteção de Dados Pessoais”, promovido pelo Ministério do Desenvolvimento, Indústria e Comércio Exterior, que dele derivou um documento chamado de “Medidas para a Proteção de dados pessoais e sua livre circulação”, incorporado em 2010 ao Mercosul. Foi quando a matéria teria sido discutida, segundo Doneda, pela primeira vez pelo Poder Executivo Brasileiro. O texto que serviu de marco a partir do debate público, com devidas contribuições posteriores, fomentou a consolidação de texto base para o Anteprojeto de Lei de Proteção de Dados pelo Ministério da Justiça. Até 2015 tal texto foi revisado e aperfeiçoado várias vezes quando sua nova versão foi tornada pública pela Secretaria Nacional do Consumidor (SENACON) ligada ao Ministério da Justiça, que por sua vez encaminhou o Anteprojeto para um debate público. O resultado foi de cerca de 1200 contribuições para enfim ser consolidado o

[32] Fonte: Agência Senado Federal (2020).
[33] MULHOLLAND, CAITLIN; NASSER, RAFAEL; CARVALHO, GUSTAVO ROBICHEZ**. A LGPD e o novo marco normativo no Brasil** / organização Caitlin Mulholland. Porto Alegre: Arquipélago, 2020, p. 7.
[34] DONEDA, 2020, Ibid., p 21-25.

texto em 2016 e enviado ao Congresso Nacional (Projeto de Lei 5.726/2016. Aprovada unanimemente no Congresso, a Lei Geral de Proteção de Dados foi promulgada em 14 de agosto de 2018).

Apesar disso, sua elaboração e sanção não foram suficientes para sua pronta entrada em vigor que foi de fato adiada por forças políticas e econômicas. Mas havia a necessidade de o Brasil integrar a Organização para a Coordenação e Desenvolvimento Econômico (OCDE). Tal Organização tinha como requisito que o país candidato tivesse um regramento de proteção de dados pessoais. [35] Considerando a questão da Organização para a Coordenação e Desenvolvimento Econômico e ainda da entrada em vigor do já citado Regulamento Geral Europeu de Proteção de Dados, fatos complementares tornaram o cenário mais propenso para a aprovação da Lei Geral de Proteção de Dados, como um verdadeiro ultimato:

> Foram eles: i) o escândalo *Cambridge Analytica*, que precipitou um debate por vezes restrito a círculos específicos para a grande mídia e o grande público; ii) a entrada em vigor, em maio de 2018, do Regulamento Geral de Proteção de Dados (RGPD) europeu, que acirrou a necessidade de maior segurança jurídica quanto ao tratamento de dados no Brasil; iii) o desejo expresso do Brasil ingressar na Organização para a Cooperação e Desenvolvimento Econômico (OCDE), que exige, como boa prática, a regulamentação de uso de dados pessoais, assim como um órgão supervisor independente e autônomo; e, por fim, iv) uma articulação interna à Câmara dos Deputados para a aprovação das alterações na Lei do Cadastro Positivo, que envolvia a aprovação da Lei Geral de Proteção de Dados como condição indispensável.[36]

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 14 de agosto de 2018) foi então aprovada em 2018 e entraria em vigor a partir de 14 de agosto de 2020. Um pedido de adiamento da vigência da lei para maio de 2021 e rejeitado pelo Congresso, fez com que a legislação entrasse em vigor em 18 de setembro de 2018, três anos depois da sua sanção, mesmo contrariando alguns setores da economia.

---

[35] BIONI, Bruno; SILVA, Paula; Pedro, Martins, 2022, Ibid., p. 27.
[36] Idem.

Se por um lado, fatores a princípio poderiam levar ao adiamento da vigência da Lei Geral de Proteção de Dados Pessoais, forçaram a sua aprovação. A pandemia da COVID -19, por outro lado, tornou sua entrada em vigor urgente em 2020, ante o surto, metaforicamente falando, do uso indiscriminado de dados pessoais e suas decorrentes violações a direitos humanos, fundamentais, do consumidor, da personalidade e direitos da livre concorrência sob o argumento de que a pandemia global justificava a emergência e calamidade pública.[37]

Era preciso traçar critérios e limites para o tratamento de dados pessoais durante a pandemia da COVID-19 que desencadeou – ou reforçou, para alguns países – o uso da tecnologia como meio de monitoramento da população. Em Taiwan e Israel, smartphones foram programados para notificar as autoridades públicas caso os pacientes perfilhados e monitorados não observassem a quarentena, em um sistema de autoridades. Na Coreia do Sul, foram divulgados os dados de viagens de 29 pacientes confirmados, compilados por meio de bases de celulares, cartões de crédito e câmeras de segurança. Nessa breve digressão, é possível perceber que o tratamento dos dados pessoais vem sendo utilizado para geolocalização, identificação e rastreamento de pacientes, gerenciamento do risco de contágio, entre outras atividades, com a finalidade de melhorar os instrumentos de combate à pandemia.[38]

Pela urgência da situação, as normas tenderam a ser flexibilizadas e as decisões governamentais sendo, muitas vezes, tomadas sem as devidas reflexões acerca do impacto na vida privada e em sociedade. O tratamento de dados deve obedecer a uma série de regras para que se garanta a tutela dos direitos à privacidade, à liberdade e à proteção dos dados pessoais, ao contrário do que se observa: a violação dos direitos dos cidadãos sob a justificativa de uma necessária escolha entre o direito à saúde ou o direito à proteção de dados pessoais.[39]

---

[37] DATA PRIVACY, 2020. Dados e o vírus. 2020 Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2020/04/Os-dados-e-o-vi%CC%81rus.pdf Acesso em: 14 de maio. 2021.

[38] SILVA; Gabriela buarque pereira; MODESTO, Jéssica andrade; JÚNIOR, marcos ehrhardt. **Direito Civil e tecnologia**. 2020, p. 167.

[39] GUIMARÃES, Arthur. Responsabilidade civil na LGPD: não há consenso entre especialistas. JOTA. 2022. Disponível em: **https://www.revistas.usp.br/rfdusp/article/download/89230/96063/167402** Acesso em: 09 de nov. de 2022.

De fato, esse foi um dos motivos para que a entrada em vigor da Lei Geral de Proteção de Dados no Brasil não significasse sua plena eficácia. Ou seja, até hoje, nos idos de 2023, a Lei Geral de Proteção de Dados Pessoais não se tornou completa realidade, mas continua a ser um grande desafio no tocante à regulamentação, aplicação e interpretação sobretudo.

Sob o olhar hermenêutico, que configura mais um obstáculo, a Lei Geral de Proteção de Dados Pessoais não é uma certeza também pelas barreiras impostas para a sua devida interpretação, pela sua integração ao ordenamento jurídico, pela aplicação e julgamento razoável por parte dos magistrados, e pelo uso da ética e da conformidade por parte das organizações.

Além disso, a busca pela fiscalização e regulamentação por órgãos administrativos, atualização e retificação oriunda do legislativo, e respeito ao cumprimento da lei pelo Poder Executivo são outros *fronts* atuais. Nessa lista, pela eficácia da norma, não se deve esquecer da imprescindibilidade da educação e conscientização da população, pois como bem rememorado, o direito não socorre aos que dormem. Esses múltiplos fatores tornam a Lei Geral de Proteção de Dados Pessoais ainda uma legislação em aberto, no sentido de vaga e em certos casos, de difícil implementação que carece do olhar de múltiplos atores. Em especial, os três Poderes executivo, legislativo e judiciário, dada a forte legitimidade destes para agir em prol da coletividade. Pois, a inovação e a tecnologia, como a própria etimologia das palavras sugere, com seu poder de predição do comportamento humano e mapeamento de tendências, tem alma bandeirante. É liberal, capitalista tendo seu maior ativo extraído do ser humano. Este em condição variável, crescente e permanente de vulnerabilidade na relação assimétrica de poder e consumo. Citam-se as relações de consumo, pois além de terem ligação direta com os objetivos desse trabalho, elas preponderam na Lei Geral de Proteção de Dados Pessoais. Estima-se que cerca de 80% por cento dos dados pessoais são de forma direta ou indireta, tratados, coletados, perfilizados a partir de situações consumeristas. Nessas relações os direitos da personalidade dos titulares de dados no contexto de avanço da tecnologia e da inovação, que são na essência a alma da Lei Geral de Proteção de Dados Pessoais, são infringidos.

Na resumida análise histórica e normativa da sequência dos acontecimentos, segue-se análise do contexto da proposta de Emenda Constitucional e a Jurisprudência do Supremo Tribunal Federal que corroboraram para sedimentar o entendimento e o reconhecimento de que a proteção de dados é um direito fundamental brasileiro e autônomo.

Esse direito foi contextualmente invocado pelas inúmeras mudanças que aconteceram no cenário tecnológico de captura de dados pessoais em afronta aos direitos fundamentais. Pois as empresas privadas demonstraram ao longo do tempo serem potencialmente mais danosas que o Estado na coleta de dados pessoais. Elas desenvolveram o método de commoditificação de dados. Perceberam que através disso conseguem maior concentração econômica e controle político. Nos elementos que fazem parte da autofagia do capitalismo de plataforma (uma expressão cunhada em 2017, pelo canadense Nick Srnicek, radicado em Londres[40], depende da colossal captura diária de dados, hoje na casa de quintilhões. Dados que se transformaram em mercadoria única (em grandes volumes, sendo, portanto, uma *commodity*). Dados capturados, armazenados, movimentados, perfilizados, demandam uma infraestrutura (plataformas) e outras condições que viabilizam o mundo digital e sua importância no capitalismo contemporâneo.

Sendo assim, temos aqui algumas das evidências de um direito novo e necessário diante dos riscos impostos aos direitos fundamentais até então positivados, face às novas tecnologias crescendo há décadas.

Avivar aqui alguns fatos faz-se necessário pois eles são fundantes e fortes argumentos baseados em necessidades crescentes da sociedade em transformação que sempre está a clamar soluções. No caso da privacidade foi preciso ampliar essa proteção de alguma forma, ao ponto de ser imprescindível um novo direito. Pois, a constitucional tutela da privacidade já não satisfazia sozinha, a proteção de dados pessoais. Reafirmando, pois, segundo Doneda, que "tal operação, se bastaria para abarcar a disciplina sob a égide constitucional, acaba por simplificar demasiadamente os fundamentos da tutela de dados pessoais, o que pode eventualmente limitar o seu alcance".[41]

---

[40] SRNICEK, Nick. **Plataform capitalism.** Cambridge: Polity Press, 2018.
[41] DONEDA, 2021, Ibid., p. 269.

Corroborando, o que se quer dizer é que várias liberdades individuais não são albergadas pelo direito à privacidade. Afastando-as assim do direito à privacidade. Nesse caso, autonomizando a proteção de dados pessoais.

A privacidade, fundamentada na divisão entre os domínios público e privado, consiste em uma liberdade negativa pela qual o indivíduo resguarda-se da interferência alheia. Em contrapartida, a proteção de dados apresenta uma característica dinâmica, proporcionando uma liberdade positiva, por meio da qual o indivíduo detém o controle das suas informações, ainda que disponibilizadas em ambiente público. [42] Assim, claramente, mesmo que deixando de lado outros aspectos, este argumento já se mostra suficiente para que a proteção de dados pessoais se tornasse um novo direito e autônomo, apartado da tutela da privacidade. Pois, o surgimento, as identificações de novos direitos fundamentais estão diretamente ligados às novas demandas da sociedade à sua época. Como afirma José Afonso da Silva, a historicidade dos direitos fundamentais "é precisamente o que lhes enriquece o conteúdo e os deve pôr em consonância com as relações econômicas e sociais de cada momento histórico".[43]

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18) também já implicitamente reclamava esse novo direito em seus sete fundamentos do seu artigo 2. O respeito à privacidade, à liberdade de expressão, à autodeterminação informativa, liberdade de informação, de comunicação e de opinião; à inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.[44]

Citar tais fundamentos da Lei Geral de Proteção de Dados é relacionar direitos essenciais que reforçam os motivos pelos quais o ordenamento jurídico pátrio reuniu esforços para inserir na Constituição Federal de maneira expressa, o direito

---

[42] BIONI, B. R. Proteção de Dados pessoais: a função e os limites do consentimento. Rio de Janeiro. Forense, 2019, p. 96-97.

[43] SILVA, José Afonso. Curso de direito constitucional positivo. 37 ed. São Paulo: Malheiros, 2013, p. 181.

[44] BRASIL, 2018. Lei nº 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Brasília, DF: Senado Federal, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 10 set. 2021.

fundamental à proteção de dados pessoais através de uma Proposta de Emenda Constitucional analisada a seguir antes de sua aprovação.

O projeto de emenda à constituição 17/19 foi aprovado na Câmara dos Deputados em agosto de 2021, em segundo turno, por maioria de 436 votos a 4, incluindo expressamente a proteção de dados pessoais na Constituição Federal do Brasil. Dessa forma, a ideia à época, era a de que fosse competência da União a função de legislar sobre o tema. Ou seja, pelo projeto de emenda à constituição, caberia à União fiscalizar e organizar essa proteção. Mas, a proposta em sua tramitação teve que retornar ao Senado para pequenas alterações em relação à inclusão de uma Autoridade Nacional Independente de Proteção de Dados expressa na Constituição.

Sobre essa Proposta de Emenda Constitucional, defendeu o Deputado Orlando Silva, relator. "Todos nós aqui utilizamos sistematicamente aplicativos na internet, e o manejo desses aplicativos se dá a partir da oferta de dados pessoais, que, muitas vezes, é objeto de manipulação sem que cada um de nós saiba os riscos à nossa privacidade", afirmou Orlando Silva.

A Ementa do projeto de emenda à constituição 17/19 formalmente na tramitação acrescentava dois incisos em dois artigos: o inciso XII-A, ao art. 5º que trata dos direitos fundamentais, e o inciso XXX, ao art. 22, estabelecendo as competências privativas da União na Constituição Federal.[45]

Pois veja-se: com esses precedentes legislativos e num cenário de transformações históricas e sociais, evidenciou- se cada vez mais o que era inescapável: a tutela constitucional da proteção de dados. O acelerador determinante e em paralelo à tramitação arrastada do projeto de emenda à constituição 17/19, estava no Supremo Tribunal Federal através da Ação Direta de Inconstitucionalidade 6.387.[46] A ADI analisava a Medida Provisória nº 954/2020. E, se antecipando ao projeto de emenda à constituição 17/19, promoveu uma decisão histórica. Na resolução do caso, a Corte proclamou o direito à proteção de dados um direito

[45] BRASIL, Senado Federal. Proposta de Emenda à Constituição n° 17, de 2019. Disponível em: < https://www25.senado.leg.br/web/atividade/materias/-/materia/135594>. Acesso em: 20 ago. 2019.
[46] BRASIL, 2020. Ação Direta de Inconstitucionalidade 6.387. Brasília, DF: Congresso Nacional, 2020. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629. Acesso em: 20 ago. 2021.

fundamental autônomo. Como um dos efeitos, essa decisão da Suprema Corte acabou por determinar urgência à tramitação da anteriormente ao projeto de emenda à constituição 17/19. Esse julgamento influenciou decisões de casos no próprio Supremo Tribunal Federal.

Rememorando os fatos do conteúdo da citada Ação Direta de Inconstitucionalidade, em abril de 2020, o governo editou a Medida Provisória n.954/2020 determinando que empresas de telecomunicação do STF e do SMP deveriam disponibilizar à Fundação IBGE, em meio eletrônico, a relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas a fim de realizar pesquisa estatística não presencial diante do isolamento populacional imposto pela pandemia.

Os ministros em seus votos, manifestaram-se pelos mais diversos motivos. Entre eles ausência de proporcionalidade, de regulação quanto aos mecanismos de segurança da informação, desnecessidade da coleta de dados milhares de brasileiros, tendo em vista realizar- se de pesquisa que precisaria apenas de amostra; além da falta de transparência para com os titulares de dados e a falta de um relatório de impacto, sendo flagrante a violação de privacidade no compartilhamento desses dados entre as empresas e o IBGE. Posto que os dados utilizados continham uma capacidade infinita de processamento. Assim, pondo em risco direitos, como se lê no trecho do voto da Ministra do Supremo, Cármen Lúcia:

> Mais do que isso, a partir de técnicas de agregação e de tratamentos, sua utilização pode-se dar para fins muito distintos dos expostos na coleta inicial, ainda sendo capazes de identificar seu titular por outras maneiras, formando, no plano virtual, perfis informacionais sobre sua personalidade. Muita vez, porém, isso se dá sem sua participação ou anuência.[47]

O voto da ministra entra em consonância com a pós-modernidade, em que a economia é baseada em dados pessoais, projeção da personalidade de cada um, sob o abrigo de garantias fundamentais. Pois este, é um recurso natural finito, ao

---

[47] BRASIL, 2020. Ação Direta de Inconstitucionalidade 6.387. Brasília, DF: Congresso Nacional, 2020. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629. Acesso em: 20 ago. 2021.

contrário dos dados que são potencialmente infinitos, porque podem ser processados, cruzados e minerados, assim como acontece no atual fenômeno do *Big Data*.

> Entende-se por uma ferramenta tecnológica capaz de processar os dados obtidos de diversas fontes e organizá-las. Na sequência, cataloga as informações e obtém um produto, que será usado estrategicamente por um sujeito nas tomadas de decisões.[48]

O que também foi levado em conta na decisão foi a recomendação da Organização Mundial de Saúde. O Regulamento Sanitário Internacional da OMS foi incorporado ao ordenamento brasileiro pelo Decreto n. 10.212, de 30 de janeiro de 2020. Tal norma determina que não devem existir "processamentos de dados desnecessários e incompatíveis" com o propósito de "avaliação e manejo de um risco para a saúde pública" (art. 45, 2, "a").[49] E embora não citada, mas que possivelmente também pode ter influenciado a decisão da Corte, foi a Convenção Interamericana de Direitos Humanos na declaração n. 01/2020, em abril de 2020. Ela considerou condenável no contexto da pandemia da Covid-19 a invasão desmedida da privacidade e do uso indevido de dados pessoais. Ou seja, posicionou-se a favor da proteção de dados e do princípio geral da não-discriminação.

> O acesso à informação verdadeira e confiável, assim como à internet, é essencial. Medidas adequadas devem ser tomadas para garantir que o uso da tecnologia de vigilância, para monitorar e rastrear a disseminação do coronavírus (Covid-19), seja limitado e proporcional às necessidades de saúde, e não envolva uma interferência desmedida e lesiva à privacidade, à proteção de dados pessoais e à observância ao princípio geral de não discriminação.[50]

---

[48] BRAGA, Jeffeson Oliveira; FERREIRA, Rafael Freire. **Direito, economia e tecnologia: ensaios interdisciplinares.** Goiânia: Editora Espaço Acadêmico, 2019.
[49] MENDES, Laura Schertel Ferreira. **Autodeterminação informativa: a história de um conceito**. Pensar. 2020, p. 63.
[50] COMISSÃO INTERAMERICANA DE DIREITOS HUMANOS. **Declaração n.01/2020**. CIDH: 2020.

Dentre os efeitos gerados pela proteção advinda da declaração de inconstitucionalidade da Medida Provisória n. 954/2020, conhecida como caso IBGE no contexto da pandemia da Covid-19, talvez o maior deles foi propiciar uma dupla proteção: como liberdade negativa do cidadão perante o Estado e ao mesmo tempo o dever de agir do Estado para garantir mecanismos de exercer esse direito.[51] De um lado, (a) essa proteção se desdobra como liberdade negativa do cidadão, oponível diante do Estado, demarcando seu espaço individual de não intervenção estatal (dimensão subjetiva). De outro lado, (b) ela estabelece um dever de atuação estatal protetiva no sentido de estabelecer condições e procedimentos aptos a garantir o exercício e a fruição desse direito fundamental (dimensão objetiva).

Dito de outra maneira, segundo o Ministro Gilmar Mendes, o conteúdo desse direito fundamental exorbita àquele protegido pelo direito à privacidade, pois não se limita apenas aos dados íntimos ou privados. Ao contrário, refere-se a qualquer dado que identifique ou possa identificar um indivíduo. Esse direito fundamental autônomo e com contornos próprios, seria extraído de uma "compreensão integrada do texto constitucional lastreada (i) no direito fundamental à dignidade da pessoa humana, (ii) na concretização do compromisso permanente de renovação da força normativa da proteção constitucional à intimidade (art. 5.º, inciso X, da CF/88) diante do espraiamento de novos riscos derivados do avanço tecnológico e ainda (iii) no reconhecimento da centralidade do habeas data enquanto instrumento de tutela material do direito à autodeterminação informativa".[52]

Mas, independentemente da decisão da Corte supra comentada, a doutrina em peso já defendia neste mesmo sentido. No de que, mesmo implicitamente, da Constituição já poderia se extrair um direito fundamental à proteção de dados pessoais. Porém, o Supremo Tribunal Federal surpreendeu mais. E foi para melhor delineamento desse direito lhe dando caráter autônomo em relação aos outros direitos fundamentais. Mesmo assim não é demais expor o posicionamento de Sarlet

---

[51] BRASIL, 2019. Proposta de Emenda à Constituição nº 17 de 2019. Acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. Brasília, DF: Senado Federal, 2019. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/135594. Acesso em: 20 set. 2021.
[52] MENDES, 2020, Ibid., p. 67.

(2020), reforçando o caráter de direito fundamental da proteção de dados pessoais anterior ao reconhecido *status* constitucional positivado:

> Já mediante uma simples leitura do catálogo que segue, enunciado nos arts. 17 e 18 da LGPD, é possível perceber que em grande medida as posições jurídicas subjetivas (direitos) atribuídas ao titular dos dados pessoais objeto da proteção legal, que concretiza e delimita, em parte, o próprio âmbito de proteção do direito fundamental à proteção de dados, coincidem com o rol de posições jurídico-constitucionais diretamente e habitualmente associadas à dupla função de tal direito como direito negativo (defesa) e positivo (a prestações). [...] A inserção de um direito à proteção de dados pessoais no texto da CF, a condição de direito fundamental autônomo não depende, em si, de tal expediente, porquanto sobejamente demonstrado que se trata de um direito implicitamente positivado, o que é objeto de amplo consenso doutrinário e mesmo acolhido na esfera jurisprudencial. um direito fundamental à proteção de dados pessoais daria maior sustentação ao marco regulatório infraconstitucional, bem como a sua aplicação pelos órgãos do Poder Judiciário, entre outras vantagens apontadas. Particularmente relevante é o fato de que a condição de direito fundamental vem acompanhada de um conjunto de prerrogativas traduzidas por um regime jurídico reforçado e uma dogmática sofisticada, mas que deve ser, em especial no caso brasileiro, desenvolvida e traduzida numa práxis que dê ao direito à proteção de dados pessoais a sua máxima eficácia e efetividade, notadamente na esfera da articulação da proteção de dados com outros direitos e garantias fundamentais e bens jurídicos e interesses de estatura constitucional. Nesse contexto, nunca é demais lembrar que levar à sério a proteção de dados pessoais é sempre também render homenagem à dignidade da pessoa humana, ao livre desenvolvimento da personalidade e à liberdade pessoal como autodeterminação.[53]

Nesse percurso, assim, após 30 anos, desde a Constituição de 1988, em 10 de fevereiro de 2022, foi promulgada pelo Congresso Nacional a Emenda Constitucional 115/2022 que inseriu expressamente a proteção de dados pessoais no rol dos

---

[53] SARLET, I. W. ; MARINONI, L. G.; MITIDIERO, D. **Curso de direto constitucional**. São Paulo: Revista dos Tribunais, 2012.

direitos fundamentais do art. 5 . da Constituição Federal através do inciso LXXIX, nos seguintes termos: "é assegurado, nos termos da lei, o direito à proteção de dados pessoais, inclusive nos meios digitais". A Emenda Constitucional ainda adicionou o inciso XXVI ao art. 21 e o inciso XXX ao art. 22 da Constituição de 1988. O que estabeleceu a competência privativa da União para legislar sobre o tema da proteção e tratamento de dados pessoais, organizar e fiscalizar a proteção e o tratamento de dados pessoais.[54]

Dessa forma, o reconhecimento desse direito foi o início de um novo horizonte de garantias e delineamento do novo direito que já vinha sendo acolhido pela doutrina, sob o manto de outras proteções constitucionais como o direito à privacidade, à intimidade e ao sigilo das comunicações, do habeas data e do princípio da dignidade humana. (TEIXEIRA, 2022, p. 246).

> Como todo direito fundamental, também o direito à proteção de dados tem um âmbito de proteção que, embora dialogue com o de outros direitos, cobre um espaço próprio e autônomo de incidência, o que se pode ilustrar mediante a referência ao fato de que a proteção de dados pessoais e o direito à privacidade e intimidade, embora zonas de convergência, são direitos fundamentais distintos. Tal âmbito de proteção é também sempre (em maior ou menor medida) - como igualmente já referido - delimitado e definido em conjunto com outros direitos e bens/interesses de hierarquia constitucional, mas também concretizado pelo legislador infraconstitucional e mesmo por decisões judiciais [...] considerando que a definição corrente e legalmente consagrada de dados pessoais - cuja consistência constitucional não tem sido objeto de relevante contestação - seja a de "informação relacionada a pessoa natural identificada ou identificável" (art. 5.°, I, da LGPD), conceito praticado também pelo RGPDE (art. 4.°, n.º 1), eventual distinção entre dados e informações parece não ser relevante do ponto de vista de sua proteção jurídico-constitucional, o que importa, ao fim e ao cabo, seria a configuração dos requisitos legais referidos, e não a forma mediante a qual se corporifica determinada informação.[55]

---

[54] BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal, 1988.
[55] SARLET, 2012, Ibid., p. 39-40.

O reconhecimento do direito fundamental à proteção de dados pessoais, assim como a sua aplicação na experiência jurídica brasileira, constitui um passo necessário para a concretização da nossa Constituição. Também a aplicação dos princípios da proteção de dados, em consonância com os modernos princípios firmados internacionalmente, representa a consolidação desse direito entre nós. Trata-se de um desenvolvimento natural do direito à privacidade, que ocorre invariavelmente a partir de novas demandas sociais originadas na sociedade da informação.[56] Consagrado o novo direito, cabem à Doutrina e à Jurisprudência encontrar formas de fortalecê-lo, protegê-lo e delimitá-lo no que ainda não foi possível.

No que concerne a sua extensão, aplicabilidade e interpretação no caso concreto, há inúmeras ações em trâmite envolvendo o tema, a exemplo as ações de controle concentrado de constitucionalidade que tramitam no Supremo Tribunal Federal: a Ação Direta de Inconstitucionalidade (ADI) 6649/DF, ajuizada pelo Conselho Federal da OAB contra o Decreto 10.046/2019 da Presidência da República, que dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados; a Ação Direta de Inconstitucionalidade 6.529/DF, com requerimento de medida cautelar, ajuizada pela Rede Sustentabilidade e pelo Partido Socialista Brasileiro contra o parágrafo único, do art. 4 da Lei 9.883/1999, que institui o Sistema Brasileiro de Inteligência, criando a Agência Brasileira de Inteligência - ABIN; e a Ação de Descumprimento de Preceito Fundamental (ADPF) 695/DE interposta pelo Partido Socialista Brasileiro (PSB), que questiona o compartilhamento de dados no âmbito da administração pública federal, em que se estima que dados de 76 milhões de brasileiros chegariam a ABIN (Agência Brasileira de Inteligência), incluindo informações como nome, filiação, endereço, telefone, dados dos veículos e fotos de todo portador de carteira de motorista no país. Todas dependem de solução a partir das decisões da Corte.

Depois de todo o exposto, constata-se que o reconhecimento do direito fundamental autônomo à proteção de dados e seu contexto, são de suma

---

[56] MENDES, G. F.; BRANCO, P. G. G. **Curso de direito constitucional**. 9. ed. São Paulo: Saraiva, 2014, p. 235-236.

importância também porque esse reconhecimento após a vigência da Lei Geral de Proteção de dados traz uma expectativa de alterações e interpretações benéficas no cenário da rede de proteção dos titulares.

CONCLUSÃO

A trajetória da Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil é um reflexo da complexidade e da urgência inerentes à proteção da privacidade e da segurança dos dados pessoais em um mundo digital em constante evolução. Ao longo deste artigo, exploramos como a LGPD, desde sua aprovação até sua entrada em vigor, moldou o cenário legal e ético em relação ao tratamento de informações pessoais no Brasil.

A pandemia da COVID-19 acelerou a necessidade de regulamentação, à medida que o uso de dados para rastreamento e controle da doença expôs desafios éticos e legais relacionados à privacidade e à vigilância. No entanto, também demonstrou a importância de um marco legal sólido que equilibre a proteção dos direitos individuais com as necessidades coletivas em momentos de crise.

O reconhecimento pelo Supremo Tribunal Federal (STF) de que a proteção de dados é um direito fundamental autônomo foi um marco importante, solidificando ainda mais a relevância da LGPD e de regulamentações similares em todo o mundo. Esse reconhecimento trouxe não apenas uma proteção legal aos cidadãos, mas também uma mudança cultural em relação à conscientização sobre a importância de controlar nossos próprios dados.

No entanto, o caminho à frente não é isento de desafios. A conformidade com a LGPD exige esforços significativos por parte das empresas e organizações, que devem adotar práticas transparentes e responsáveis de tratamento de dados. Além disso, a sociedade precisa continuar debatendo as questões éticas e legais que surgem à medida que a tecnologia avança.

A LGPD representa uma conquista importante na proteção da privacidade e dos direitos individuais no Brasil. No entanto, é apenas o começo de uma jornada mais longa em direção a um ambiente digital mais seguro e ético. À medida que

novas tecnologias emergem e desafiam nossas concepções tradicionais de privacidade, a adaptação constante das leis e regulamentos se torna essencial.

Em última análise, a LGPD destaca a necessidade de encontrar um equilíbrio entre a inovação tecnológica e a proteção dos direitos humanos fundamentais. É um lembrete de que, em um mundo orientado por dados, a privacidade e a segurança dos cidadãos devem permanecer no centro de nossas preocupações. A jornada rumo à proteção de dados pessoais é contínua e exige a colaboração de governos, empresas e cidadãos para assegurar um futuro digital mais justo, transparente e seguro para todos.

REFERÊNCIAS

BIONI, Bruno Rodrigues. **Proteção de Dados Pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019.

BIONI, Bruno; SILVA, Paula; MARTINS, Pedro. **Intersecções e Relações entre a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI): Análise Contextual pela Lente do Direito de Acesso**. In: Coletânea de artigos da pós-graduação em ouvidoria pública, 2022. Disponível em: https://revista.cgu.gov.br/Cadernos_CGU/article/view/504/284. Acesso em: 16 nov. 2022.

BRAGA, Jeffeson Oliveira; FERREIRA, Rafael Freire. **Direito, Economia e Tecnologia: Ensaios Interdisciplinares**. Goiânia: Editora Espaço Acadêmico, 2019.

BRASIL. Projeto de Lei 4.365 de 1977. Brasília: Diário do Congresso Nacional, 1977. Disponível em: **https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=FBF15270DD557906FEB1829EFEA68AED.proposicoesWeb1?codteor=1172300&filename=Avulso+-PL+2796/1980**. Acesso em: 10 nov. 2020.

BRASIL. Projeto de Lei 2.796 de 1980. Brasília: Diário do Congresso Nacional, 1980. Disponível em: **https://imagem.camara.gov.br/Imagem/d/pdf/DCD23ABR1980.pdf#page=19**. Acesso em: 10 nov. 2020.

BRASIL. Lei 824 de 1984. Assegura o direito de obtenção de informações pessoais contidas em bancos de dados operando no estado do Rio de Janeiro e dá outras providências. Brasília, 1984. Disponível em: **https://gov-rj.jusbrasil.com.br/legislacao/149858/lei-824-84**. Acesso em: 10 ago. 2022.

BRASIL. Lei 8.078 de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: **http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm**. Acesso em: 10 ago. 2020.

BRASIL. Decreto 6.659, de 2008. Disponível em: **http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Decreto/D6659.htm**. Acesso em: 14 de maio. 2021.

BRASIL. Proposta de Emenda Constitucional 17 de 2019. Acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. Brasília, DF: Senado Federal, 2019. Disponível em: **https://www25.senado.leg.br/web/atividade/materias/-/materia/135594**. Acesso em: 20 set. 2021.

BRASIL, 2021. Acesso à informação não pode ser prejudicado por conta de Lei de Proteção de Dados, dizem especialistas. Agência Câmara de Notícias. Disponível em: **https://www.camara.leg.br/noticias/828370-acesso-a-informacao-nao-pode-ser-prejudicado-por-conta-de-lei-de--protecao-de-dados-dizem-especialistas**. Acesso em: 5 set. 2022.

CIDH. **Comissão Interamericana De Direitos Humanos**. Declaração 01/2020. CIDH: 2020.

CRUZ, Francisco Carvalho de Brito. **Direito, Democracia e Cultura Digital: A Experiência de Elaboração Legislativa do Marco Civil da Internet**. Dissertação (Mestrado em Direito) - Faculdade de Direito da Universidade de São Paulo. São Paulo, 2015. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2139/tde-08042016-154010/publico/dissertacao_Francisco_Carvalho_de_Brito_Cruz.pdf. Acesso em: 3 ago. 2022.

DALLARI, Dalmo de Abreu. **Direitos Humanos e Cidadania**. São Paulo: Moderna, 2002.

DATA PRIVACY, 2020. Dados e o Vírus. 2020. Disponível em: **https://www.dataprivacybr.org/wp-content/uploads/2020/04/Os-dados-e-o-vi%CC%81rus.pdf**. Acesso em: 14 de maio. 2021.

DECLARAÇÃO de Santa Cruz de La Sierra documento final da XIII Cumbre Ibero-Americana de Chefes de Estado e de Governo, disponível em: **https://www.segib.org/wp-content/uploads/DECLARASAO-STA-CRUZ-SIERRA.pdf**. Acessado em março de 2021.

DONEDA, Danilo; MENDES, Laura Shertel. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021.

DONEDA, Danilo. **Lei geral de proteção de dados (Lei 13.709/2018) a caminho da efetividade: contribuições para a implementação da LGPD**. São Paulo: Thomson Reuters, 2020.

GREENLEAF, G. Global Data Privacy Laws. 120 National Data Privacy Laws, Including Indonesia and Turkey. Privacy Laws & Business International. 2017. Disponível em: **https://ssrn.com/abstract=2993035**. Acesso em: 03 abr. de 2022.
GUIMARÃES, Arthur. Responsabilidade civil na LGPD: não há consenso entre especialistas. JOTA. 2022. Disponível em: **https://www.revistas.usp.br/rfdusp/article/download/89230/96063/167402**. Acesso em: 09 de nov. de 2022.

IDEC, 2018. Após Pressão da Sociedade, Senado Aprova Lei de Dados Pessoais. Disponível em: **https://idec.org.br/noticia/apos-pressao-da-sociedade-senado-aprova-lei-de-dados-pessoais**. Acesso em: 10 nov. 2020.

MENDES, G. F.; BRANCO, P. G. G. **Curso de Direito Constitucional**. 9. ed. São Paulo: Saraiva, 2014.

MENDES, Laura Schertel Ferreira. **Autodeterminação Informativa: a História de um Conceito**. Pensar. 2020.

MMA, 2022. Sobre o MMA. 2022. Disponível em: **https://www.mmaglobal.com/files/documents/copia_de_mma-playbook-privacy_2018_pt-3.pdf**. Acesso em: 10 nov. 2020.

MULHOLLAND, CAITLIN; NASSER, RAFAEL; CARVALHO, GUSTAVO ROBICHEZ. **A LGPD e o Novo Marco Normativo no Brasil**. Organização Caitlin Mulholland. Porto Alegre: Arquipélago, 2020.

NIC.BR, 2018. Como Robôs Influenciaram as Eleições de 2014 no Brasil. Disponível em: **https://nic.br/noticia/na-midia/como-robos-influenciaram-as-eleicoes-de-2014-no-brasil/**. Acesso em: 10 nov. 2020.

SARLET, I. W. ; MARINONI, L. G.; MITIDIERO, D. **Curso de Direito Constitucional**. São Paulo: Revista dos Tribunais, 2012.

SILVA, José Afonso. **Curso de Direito Constitucional Positivo**. 37 ed. São Paulo: Malheiros, 2013.

SILVA; Gabriela Buarque Pereira; MODESTO, Jéssica Andrade; JÚNIOR, Marcos Ehrhardt. **Direito Civil e Tecnologia**. 2020.

SRNICEK, Nick. **Plataform Capitalism**. Cambridge: Polity Press, 2018.

TOMASEVICIUS FILHO, Eduardo. Em direção a um novo 1984? A tutela da vida privada entre a invasão de privacidade e a privacidade renunciada. R. Fac. Dir. Univ.

São Paulo v. 109 p. 129 - 169 jan./dez. 2014. Disponível em: **https://www.revistas.usp.br/rfdusp/article/download/89230/96063/167402**. Acesso em: 14 de maio. 2021.

WALD, Arnoldo. **O Habeas Data na Lei 9.507/97**. In: WAMBIER, Teresa Arruda Alvim (Coord.). Habeas Data. São Paulo: Revista dos Tribunais, 1998.

3. O SISTEMA EUROPEU DE PROTEÇÃO DE DADOS: UMA JORNADA DE EMPODERAMENTO DO INDIVÍDUO

https://doi.org/10.36592/9786554600798-03

Debora Sirotheau Siqueira Rodrigues[1]

Martha Leal[2]

RESUMO

O artigo discorrerá sobre a evolução do direito a proteção de dados no sistema europeu, abordando os diferentes níveis de leis, desde a primeira legislação no tema, oriunda da lei de lande de Hesse, passando pela Convenção 108, até a entrada em vigor do Regulamento Geral de Proteção de Dados e a sua influência na legislação brasileira, bem como no contexto regulatório mundial. Destacar-se-á a relevância da ascensão do direito à proteção de dados na União Europeia e seus impactos na sociedade econômica, que passou a exigir novas formatações de desenvolvimento de atividades comerciais, a fim de que as empresas se adequassem às exigências trazidas por um arcabouço de normas legais. Por fim, o presente ensaio pretende ressaltar a importância do respeito à pessoa humana, como centro do desenvolvimento do direito à proteção de dados pessoais.

Palavras-chave: empoderamento do indivíduo; desenvolvimento tecnológico; livre fluxo informacional; proteção de dados; sistema europeu.

1. INTRODUÇÃO

Vivemos numa sociedade onde a tecnologia da informação, *big data*[3] e consumo de dados é uma realidade imutável nas nossas vidas, tendo provocado

---

[1] Advogada com pós-graduação em Privacidade e Proteção de Dados. Analista de TI com pós-graduação em Redes de Computadores. Certificada CIPM e CDPO/BR pela IAPP. Membro do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade- CNPD, órgão consultivo da Autoridade Nacional de Proteção de Dados - ANPD. Vice-presidente da Comissão Especial de Proteção de Dados da OAB Nacional. Presidente da Comissão Estadual de Proteção de Dados da OAB/PA. Conselheira Seccional da OAB/PA. Membro das Comissões de Relações Institucionais e de Relações do Trabalho do Instituto Nacional de Proteção de Dados – INPD.

[2] Advogada Especialista em Proteção de Dados. Advogada especialista em proteção de dados. Pós-graduada em Direito Digital pela Fundação Superior do Ministério Público do Rio Grande do Sul. Mestre em Direito e Negócios Internacionais pela Universidad Internacional Iberoamericana Europea del Atlântico e pela Universidad UNINI México. Pós-graduada em Direito Digital pela Universidade de Brasília - IDP. Data Protection Officer ECPB pela Maastricht University. Certificada como Data Protection Officer pela EXIN. Certificada como Data Protection Officer pela Fundação Getúlio Vargas do Rio de Janeiro - FGV. Mestranda na Unisinos – Mestrado Profissional em Direito. Presidente da Comissão de Comunicação Institucional do Instituto Nacional de Proteção de Dados – INPD. E-mail: marta@jpleal.com.br.

[3] (**Megadados** ou **grandes dados** em português) é a área do conhecimento que estuda como tratar, analisar e obter informações a partir de conjuntos de dados grandes demais para serem analisados

profundas alterações na economia mundial, no nosso dia a dia, na forma como nos relacionamos pessoalmente e profissionalmente, nos trazendo uma infinidade de oportunidades até pouco tempo impensadas pela distância física de nos fazermos presentes e que acabou permitindo uma melhor democratização nas relações.

A dinâmica de nossas rotinas foi alterada substancialmente em decorrência do desenvolvimento tecnológico, nos permitindo um universo de interações e informações digitais onde a velocidade e o alcance da informação nos mostrou a face positiva e negativa da extrema exposição de nossas vidas privadas e públicas. Tal cenário nos impõem o reconhecimento das possibilidades que nos foram ofertadas, sem, no entanto, nos descuidarmos dos desafios que a realidade digital nos apresenta e a dimensão da esfera pública e privada, que a cada vez, parece estar mais ameaçada.

Desta feita, sem desconsiderar os benefícios trazidos pelo desenvolvimento das novas tecnologias em informática, o uso de uma rede mundial de computadores, o avanço da inteligência artificial, os quais já incorporamos de tal forma em nossa rotina que seria quase impossível nos imaginarmos sem os mesmos, bastando referir singelos exemplos, como a possibilidade de falarmos com uma pessoa que está a quilômetros de distância, em tempo real, obter conhecimento, notícias de interesse próprio ou profissional a custo zero ou ínfimo, trabalharmos remotamente sem sairmos de nossas próprias casas, acessar nossas contas bancárias, obter atendimento médico por meio de telemedicina e que são apenas alguns dos

---

por sistemas tradicionais. Ao longo das últimas décadas, a quantidade de dados gerados tem crescido de forma exponencial. O surgimento da Internet aumentou de forma abrupta a quantidade de dados produzidos, e a popularização da Internet das coisas fez sairmos da era do terabyte para o petabyte. Em 2015, entramos na era do zetabytes, e atualmente geramos mais de 2,5 quintilhões de bytes diariamente. O termo *Big Data* surgiu em 1997 e seu uso foi utilizado para nomear essa quantidade cada vez mais crescente e não estruturada de dados sendo gerados a cada segundo. Atualmente o *big data* é essencial nas relações econômicas e sociais e representou uma evolução nos sistemas de negócio e na ciência. As ferramentas de *big data* são de grande importância na definição de estratégias de marketing, aumentar a produtividade, reduzir custos e tomar decisões mais inteligentes. A essência do conceito está em gerar **valor** para negócios. No que tange a ciência, o surgimento do *big data* representou a criação de um novo paradigma (4° paradigma) sendo concebido um novo método de avançar as fronteiras do conhecimento, por meio de novas tecnologias para coletar, manipular, analisar e exibir dados, construindo valor agregado com as análises geradas. BIG DATA. *In:* WIKIPÉDIA. Wikimedia Foundation. 2020. Disponível em: https://pt.wikipedia.org/wiki/Big_data. Acesso em: 03 out. 2023 (grifo nosso).

incontáveis benefícios os quais passamos a usufruir e que indubitavelmente, nos trouxeram mais tempo e maior qualidade de vida.

Surgiu assim um novo ambiente virtual, denominado de “ciberespaço”, o qual se traduz no espaço de comunicação onde ocorre a interconexão dos computadores, que inclui a transmissão de todas as comunicações digitais.

Esse novo terreno onde as relações entre os indivíduos da sociedade passam a se desenrolar na esfera pessoal e profissional requer sem sombra de dúvida um olhar mais atento aos impactos decorrentes da velocidade de propagação de uma informação e a sua escalabilidade, independentemente de fronteiras físicas.

E é a partir da premissa incontestável de que o fluxo de informações de ordem pessoal, agregados a ampla capacidade de processamento atual da tecnologia representa um panorama irreversível, reconhecendo os seus benefícios e potenciais riscos à privacidade e proteção de dados, que o presente artigo pretende repassar o histórico do direito à proteção de dados no cenário europeu para compreensão de que desde as primeiras normas existentes, os seus nascimentos foram provocados pelos desafios impostos pela tecnologia.

2. DOS DIFERENTES NÍVEIS DE LEIS

Importante contextualizarmos o desenvolvimento das leis protetivas de dados pessoais, no cenário internacional, para que possamos compreender melhor a evolução do tema. Conforme bem preceitua Laura Schertel[4] podemos considerar a existência de diferentes níveis de legislações.

Os diferentes estágios das normas protetivas de dados pessoais seriam representados por cinco gerações a seguir detalhadas:

a. a primeira geração teria nascido, na década de 1970, em resposta ao uso de dados na administração pública e empresas privadas e a criação de um banco de dados centralizado para uso da máquina estatal;

---

[4] MENDES, **Laura Schertel**. *A lei* ***geral de proteção de dados*** *pessoais: um modelo de aplicação em três níveis*. Caderno Especial LGPD. São Paulo: RT**, 2019.**

b. a segunda geração sobreveio em decorrência da transformação tecnológica que permitiu que tanto o governo como a iniciativa privada processassem dados pessoais de forma descentralizada, acarretando o aumento dos bancos de dados e a necessidade de uma regulamentação que priorizasse os direitos à privacidade, às liberdades individuais, às liberdades negativas e à liberdade individual em geral, dos titulares, em detrimento de procedimentos legais. Aqui, há a substituição do receio de um banco de dados único e centralizado pela ameaça da existência de diversos bancos de dados espalhados mundialmente e conectados em rede e os riscos advindo de seus gerenciamentos;

c. a terceira geração de normas de proteção de dados pessoais surge em 1983, com a declaração pelo Tribunal Constitucional Alemão, que declarou a inconstitucionalidade parcial da Lei do Censo[5], explicitando-se, assim, pela primeira vez o direito à autodeterminação informativa. Os indivíduos passam a ter o poder de decidir sobre questões de coleta, divulgação e uso de seus dados pessoais;

d. a quarta geração de normas foi provocada pela falta de engajamento da sociedade no controle efetivo de suas informações frente aos custos monetários e sociais de fazerem valer este direito, agregado aos custos da privação de bens e serviços que lhe eram impostos por assim agirem.[6] Assim, buscou-se dar maior poder ao indivíduo sobre os seus dados por meio de um controle individual mais efetivo, ao mesmo tempo em que, extraiu-se da esfera exclusivamente individual temas considerados de extrema relevância e que pela sua natureza requerem proteção extra, justificando a não restrição no âmbito individual. A proibição imposta ao tratamento de dados sensíveis, de forma parcial ou integral, tendo em vista o potencial de riscos discriminatórios tais como etnia, opção sexual, opinião política e religião ilustra o alcance do tema na esfera pública;

e. por fim, admite-se estarmos vivenciando a quinta geração de proteção de dados, provocada pela revisão das Diretrizes por parte da OCDE de 2013, a edição do Regulamento Geral de Proteção de Dados na UE que entrou em eficácia plena em 25 de maio de 2018 e demais leis de proteção de dados aprovadas no cenário

---

[5] BVFGE 65; VOLKSZAHLUNG *apud* MARTINS, Flávio. *Curso de direito constitucional***.** São Paulo: Saraiva, 2005.

[6] BVFGE 65; VOLKSZAHLUNG *apud* MARTINS, Flávio. *Curso de direito constitucional***.** São Paulo: Saraiva, 2005.

mundial, a exemplo da Lei de Proteção de Dados da Califórnia. Na presente etapa, além do controle do indivíduo passa-se a atribuir responsabilidade a toda cadeia de agentes de tratamento, amparado no princípio da *accountability*.

3. DA EVOLUÇÃO DAS LEIS DE PROTEÇÃO DE DADOS

O primeiro registro da proteção de dados no cenário europeu teve origem na Lei do Estado alemão de Hesse, a denominada Lei de Hesse, editada no ano de 1970.

Segundo o autor Fabiano Menke[7], a Lei de Hesse, na sua versão original, contemplou apenas dezessete parágrafos distribuídos em três capítulos, muito diferente da lei atualizada, a qual contêm cinco capítulos e noventa e um parágrafos.

A lei original estabelecia regras na esfera pública do Estado de Hesse, sobre o que denominava de "área de proteção de dados" e fixava a abrangência da lei para todos os documentos confeccionados por meio de processamento automatizado de dados, para os dados armazenados e para o resultado do seu processamento.

A norma também inovou ao estipular em seu parágrafo segundo, sob o título de "conteúdo da proteção de dados" a obrigatoriedade de que os documentos, dados e resultados de diagnósticos dos pacientes deveriam receber medidas técnicas aptas para que pessoas não autorizadas ficassem impedidas de acessar, alterar ou eliminar as informações, garantindo a integridade e evitando a perda dos documentos.

Havia expressa referência ao dever de confidencialidade das pessoas envolvidas no tratamento das informações sobre as quais a lei incidia, bem como, previa em seu parágrafo quarto, o dever do controlador em corrigir dados armazenados e que dizem respeito ao titular, assemelhando-se, mesmo que de forma embrionária, aos direitos reconhecidos aos titulares de dados pessoais pelas legislações atuais.

---

[7] MENKE, Fabiano. Spiros Simitis e a primeira lei de proteção de dados do mundo. **Migalhas,** 19 nov. 2021. Disponível em: http://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/355182/spiros-simitis-e-a-primeira-lei-de-proteçao-de-dados-do-mundo. Acesso em: 03 out. 2023.

De forma pioneira, a norma legal estabeleceu a figura da autoridade pela proteção de dados, a exemplo do *Data Prottection Officer*, na legislação europeia, e encarregado na legislação nacional.

No modelo alemão, a figura que desempenha este papel detém autonomia e é escolhida pelo Parlamento Estadual para exercer as funções.

Cabe registrar que a lei em questão representou uma iniciativa de regular a limitação da manipulação dos dados pessoais, à época, contra o uso abusivo da administração pública estatal.

Segundo o autor Danilo Doneda[8]:

> Tais iniciativas refletem o estado da tecnologia e a visão do jurista à época, notadamente vinculada à experiência do *National Data Center* e similares, marcada pela convicção de que direitos e liberdades fundamentais estariam ameaçados pela coleta ilimitada de dados pessoais, uma operação que então era realizada basicamente pelo Estado. Tais leis são conhecidas hoje como leis de primeira geração em proteção de dados pessoais, em uma classificação habitualmente utilizada pela doutrina.

O propósito da Lei de Hesse era a regulação da manipulação excessiva de dados por determinados atores, no caso o Estado, refreando este uso através da implementação de controles no uso das informações, atribuindo regras específicas aos responsáveis pelo tratamento de dados.

E, sem sombra de dúvidas, o status do ambiente tecnológico foi determinante para que este primeiro grupo de normas legais não lograsse êxito em acompanhar o elevado número de banco de dados que surgiam, na medida em que o formato pautado na exigência de autorizações demandava um trabalho hercúleo por parte dos responsáveis pelo controle de acessos.

Em um segundo momento legislativo, surge a lei francesa de proteção de dados, a *Liberté e Informatique*, de 1978, e que previa também um controle público e privado para a manipulação automatizada de dados pessoais por meio de

---

[8] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006. p. 207.

mecanismo de registro que se perfectibilizava através de uma comissão de controle estatal.

A terceira fase da legislação de proteção de dados surge dentro de um ambiente de percepção da importância da informação como extensão da personalidade e a consequente importância da sua proteção na esfera da privacidade.

E é nesse cenário que surge a importante decisão proferida pelo Tribunal Constitucional Alemão e que julgou em 1983 a inconstitucionalidade da lei do Censo e que determinava o recenseamento geral da população e o amplo compartilhamento dos dados pessoais da população com os órgãos administrativos.

O controle individual sobre os dados foi trazido pela primeira vez nesta decisão proferida, no caso do censo populacional inaugurando o conceito de autodeterminação informacional, elemento fundamental para a garantia dos direitos individuais.[9]

A referida lei exigia que os dados sobre profissão, endereço residencial e profissional dos cidadãos fossem disponibilizados ao Estado para fins de apuração do status de crescimento populacional, além de características demográficas e sociais. A norma legal também autorizava que o Estado fizesse um cruzamento das informações dos indivíduos com as constantes nos registros públicos, com a finalidade de obtenção de um cadastro completo dos cidadãos.

A proteção de dados, influenciada pela decisão do Tribunal Constitucional Alemão passou a ter status constitucional ao anunciar o direito fundamental ao livre desenvolvimento da personalidade e da dignidade humana.

A participação do indivíduo na sociedade e o contexto em que ele está inserido, onde os seus dados são exigidos como condicionante para que tenha uma participação no ambiente social e econômico passam a ser considerados, estabelecendo-se, consequentemente, mecanismos de proteção para salvaguardar o efetivo exercício da autodeterminação informativa.

Nesse sentido, Doneda assim se manifestou:

---

[9] HORNUNG, Gerrit; SCHNABEL, Christoph. Data Protection in Germany I: the population census decision and the right to informational self-determination. **Computer Law and Security Review,** Kassel, n. 25, p. 84-88, 2009.

> A autodeterminação informativa, de fato, surgiu basicamente como uma extensão das liberdades pressentes nas leis de segunda geração, e são várias as mudanças específicas nesse sentido que podem ser identificadas na estrutura destas novas leis. O tratamento dos dados pessoais era visto como o processo que não se encerrava na simples permissão ou não da pessoa para a utilização dos seus dados pessoais, porém procurava fazer com que a pessoa participasse consciente e ativamente nas fases sucessivas do processo de tratamento e utilização de sua própria informação por terceiros; estas leis incluem também garantias específicas, como o dever de informação.[10]

4. A CONVENÇÃO 108 E A SUA RELEVÂNCIA PARA A PROTEÇÃO DE DADOS

A Convenção 108 do Conselho da Europa, instituída em 1981 em Estrasburgo, na França é o primeiro e único tratado internacional juridicamente vinculativo e que trata da privacidade e da proteção de dados pessoais, sendo até os dias de hoje, consagrado como um dos mais relevantes instrumentos envolvendo o tema globalmente.[11]

O referido instrumento, conhecido como a Convenção 108, versa sobre a proteção das pessoas singulares no que diz respeito ao tratamento automatizado de dados pessoais e tem como objetivo garantir a todas as pessoas o respeito a direitos e liberdades fundamentais, em especial à vida privada, face ao processamento automatizado de dados pessoais.[12]

Através da Convenção 108, o Conselho da Europa reconheceu que a proteção à privacidade e aos dados pessoais são fundamentais à manutenção dos direitos dos homens, estando disponível para adesão por países europeus e não europeus.

---

[10] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* Rio de Janeiro: Renovar, 2006. p. 211-212

[11] CONSELHO DA EUROPA. *Convenção para a proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal (Convenção 108)* de 28 de janeiro de 1981. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108. Acesso em: 03 out. 2023.

[12] CONSELHO DA EUROPA. *Convenção para a proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal (Convenção 108)* de 28 de janeiro de 1981. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108. Acesso em: 03 out. 2023.

Em 2018, o Conselho da Europa propôs a modernização da Convenção 108 (Convenção 108+)[13] adaptando o texto original às novas tecnologias de informação e comunicação possibilitando uma maior efetividade na implementação.

Posteriormente a Convenção 108, nos anos 2000, a União Europeia reconheceu a proteção de dados como direito fundamental.

5. A DIRETIVA DE PROTEÇÃO DE DADOS (DIRETIVA 95/46/CE) E A BUSCA PELA HARMONIZAÇÃO LEGISLATIVA NO BLOCO EUROPEU

No início dos anos 90, poucos países haviam ratificado a Convenção 108 e incorporado nos seus respectivos ordenamentos jurídicos as regras de proteção de dados contidas nesse importante instrumento internacional. Ademais, os países que haviam adotado leis de proteção de dados, não seguiram uma mesma abordagem legislativa.

Desta feita, considerando as diferentes abordagens que as leis nacionais dos Estados-membros estavam adotando para a temática da proteção de dados e buscando harmonizá-las para facilitar a abertura do mercado interno e a livre circulação de mercadorias, pessoas, serviços, capitais, e, consequentemente, dados pessoais, a Comissão Europeia foi instada pelo Parlamento Europeu a elaborar uma proposta de Diretiva que assegurasse aos indivíduos um nível de proteção adequado diante do tratamento dos seus dados pessoais, de modo que os dados pudessem fluir livremente, propiciando o desenvolvimento econômico do mercado interno.

Vale ressaltar que a Diretiva é um tipo de legislação que, muito embora vincule os Estados-membros, não é diretamente aplicável, necessitando de um processo de transposição para as legislações nacionais, deixando a cargo de cada país a escolha sobre a forma e métodos de sua implementação.

Como ponto de partida para a elaboração da Diretiva sobre Proteção de Dados, a Comissão Europeia baseou-se nos princípios de proteção de dados contidos na Convenção 108, do Conselho da Europa, tendo em vista que eles estavam presentes,

---

[13] COUNCIL OF EUROPE. Convention for the protection of individuals with regard to the processing of personal data (CETS 108). In:– COE. 2018. Disponível em: https://rm.coe.int/cahdata-convention-108-table-e-april2018/16808ac958. Acesso em: 03 out. 2023..

como uma espécie de conjunto padrão, em todos os países que a haviam ratificado. Vale mencionar que essa escolha legislativa se repetiu ao longo do tempo, sendo perceptível que a maioria das legislações atualmente existentes foram estruturadas sobre essas mesmas bases principiológicas.

Alguns anos depois, mais precisamente em 24 de outubro de 1995, foi adotada a Diretiva 95/46/CE, do Parlamento Europeu e do Conselho, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.[14]

Importa mencionar que a Diretiva, ao prever a proteção tanto para o tratamento automatizado como para o tratamento não automatizado de dados pessoais, com aplicação para os setores público e privado, alargou o escopo de proteção previsto na Convenção 108.

De forma geral, pode-se afirmar que a Diretiva 95/46 fortaleceu as regras de proteção de dados pessoais até então existentes ao trazer em seu texto uma série de inovações como a previsão de uma ou mais autoridades públicas de proteção de dados (DPAs) responsáveis pela fiscalização da aplicação das disposições adotadas pelos Estados-membros, quando da transposição da Diretiva para as legislações nacionais, com garantia de total independência no desempenho de suas funções. A atuação das autoridades independentes de proteção de dados, foi, sem nenhuma dúvida, de fundamental importância para a correta aplicação da lei.

Em comparação com a Convenção 108, a Diretiva trouxe uma quantidade e clareza maior de conceitos, tais como o conceito de dados pessoais, de tratamento de dados e de responsável pelo tratamento de dados, apenas para citar alguns desses importantes conceitos relacionados ao tema que necessitavam de uma definição legal. Ademais, estabeleceu uma lista exaustiva de bases legais para legitimar o tratamento de dados pessoais, diferenciando as hipóteses aplicáveis ao tratamento de dados não sensíveis das hipóteses para o tratamento de dados sensíveis, na intenção de buscar uma maior harmonização entre as leis dos Estados-membros.

---

[14] DIRECTIVA 95/46/CE DO PARLAMENTO EUROPEU E DO CONSELHO relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados de 24 de outubro de 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046. Acesso em: 04 out. 2023.

A Diretiva também inovou ao ampliar os direitos dos titulares já previstos na Convenção 108, além de introduzir novos, assegurando um maior controle das pessoas sobre o fluxo de seus dados, o que resultou em um empoderando dos indivíduos diante do tratamento de seus dados.

A segurança do tratamento também foi fortalecida, sendo imposta ao responsável pelo tratamento a obrigação de adotar medidas técnicas e organizativas adequadas para proteção dos dados pessoais contra a destruição acidental ou ilícita, a alteração, a difusão ou acesso não autorizados, bem como contra qualquer outra forma de tratamento ilícito, garantindo um nível de segurança adequado em relação aos riscos que o tratamento apresentasse e à natureza dos dados tratados. Além de que, o responsável pelo tratamento, ao escolher um subcontratante, deveria assegurar que ele oferecesse garantias suficientes em relação às medidas de segurança do tratamento, estando obrigado a firmar com ele um contrato ou ato jurídico, por escrito ou outra forma equivalente, que estabelecesse as respectivas obrigações em relação à segurança dos dados e garantisse a observância das instruções fornecidas pelo responsável ao subcontratante, para o tratamento dos dados em questão.

Uma outra previsão importante trazida pela Diretiva refere-se às medidas necessárias para assegurar a proteção de dados pessoais nas transferências internacionais de dados para os países que não fazem parte do Espaço Econômico Europeu, os chamados países terceiros, previsão que a Convenção 108 não trouxe, deixando sob a responsabilidade de cada país o estabelecimento dessas regras.

Como visto, são muitos os elementos introduzidos pela Diretiva de Proteção de Dados, como, por exemplo, a criação do Grupo de Trabalho do artigo 29 (Article 29 Working Party - WP29), previsto no artigo 29 da respectiva Diretiva. O WP29 era composto por representantes das autoridades independentes de proteção de dados dos Estados-membros, por representantes do EDPS,[15] além de um representante da

[15] O European Data Protection Supervisor (EDPS) ou Autoridade Europeia para a Proteção de Dados (AEPD) é a autoridade independente de proteção de dados da União Europeia dotada de poderes de supervisão que tem como uma de suas funções assegurar que as instituições e órgão comunitários observem o direito à proteção de dados pessoais sempre que realizarem atividade de tratamento de dados pessoais. Disponível em: https://edps.europa.eu/about-edps_en?etrans=pt. Acesso em: 04 out. 2023.

Comissão Europeia, este sem direito a voto, e tinha como objetivo principal a harmonização na aplicação da Diretiva, especialmente através da adoção de recomendações e opiniões. Nesse sentido, o WP29 produziu um elevado número de documentos sobre diversos assuntos relacionados com a aplicação da Diretiva 95/46, que apesar de não vinculantes, eram extremamente respeitados e contribuíram sobremaneira para mitigar os problemas oriundos das divergências nas legislações nacionais dos Estados-membros.

Contudo, com passar do tempo, percebeu-se que as diferenças existentes nas legislações nacionais, em decorrência do processo de transposição da Diretiva, estavam criando empecilhos para o desenvolvimento dos negócios, que não estavam conseguindo usufruir dos benefícios de um mercado interno, problema reportado no Relatório da Comissão Europeia sobre a Diretiva, publicado no ano de 2004[16] e, como será visto adiante, um dos motivos para a aprovação do Regulamento 2016/679 (Regulamento Geral de Proteção de Dados - RGPD)[17], instrumento normativo que substituiu a Diretiva de Proteção de Dados.

Dentre as inconsistências encontradas nas legislações dos Estados-membros, podemos citar, como exemplo, o processo de notificação do tratamento de dados às autoridades supervisoras (DPAs). Os requisitos para essa notificação variavam bastante entre as diversas legislações nacionais, o que trazia dificuldade para as organizações, em decorrência do aumento dos encargos administrativos para cumprir com diferentes requisitos legais, problema que era majorado quando as organizações possuíam relações comerciais também com países terceiros.

---

[16]COMISSÃO EUROPEIA. *Relatório Geral sobre a Actividade da União Europeia — 2003 adotado pela Comissão Europeia em 23 de Janeiro de 2004*, p. 109. Disponível em: https://eur-lex.europa.eu/resource.html?uri=cellar:ba77533a-9d00-4687-b77f-a7e598000175.0004.02/DOC_2&format=PDF. Acesso em: 04 out. 2023.

[17] PARLAMENTO EUROPEU. *REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016*. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 04 out. 2023.

6. O REGULAMENTO GERAL DE PROTEÇÃO DE DADOS: UMA EVOLUÇÃO DO SISTEMA EUROPEU DE PROTEÇÃO DE DADOS EM BUSCA DE MAIOR COERÊNCIA E ROBUSTEZ

Além da ausência de uma legislação harmônica entre os Estados-membros da União Europeia, em decorrência das diferenças na transposição da Diretiva 95/46/CE para as legislações nacionais, conforme já mencionado, a Diretiva, embora tecnologicamente neutra, necessitava de atualização, tendo em vista que foi concebida antes do acesso massivo à internet, antes da era do *big data*[18], do uso da inteligência artificial, das decisões algorítmicas, dentre outras mudanças tecnológicas que ocorreram desde sua aprovação, em outubro de 1995.

De fato, o desenvolvimento tecnológico promoveu uma mudança drástica na forma como os dados pessoais passaram a ser coletados, acessados e utilizados, sendo urgente garantir a proteção dos indivíduos em face dos riscos aos seus direitos e garantias fundamentais que o tratamento de dados pessoais representa nesse novo contexto tecnológico.

Em 2012, diante da necessidade cada vez maior de uma harmonização entre as legislações, bem como de sua modernização, a Comissão Europeia, visando garantir uma maior proteção e controle dos indivíduos sobre seus dados, diante dos novos desafios econômicos e sociais impostos pela era digital, propôs uma atualização na legislação vigente, na forma de um Regulamento Geral de Proteção

[18] (**Megadados** ou **grandes dados** em português) é a área do conhecimento que estuda como tratar, analisar e obter informações a partir de conjuntos de dados grandes demais para serem analisados por sistemas tradicionais. Ao longo das últimas décadas, a quantidade de dados gerados tem crescido de forma exponencial. O surgimento da Internet aumentou de forma abrupta a quantidade de dados produzidos, e a popularização da Internet das coisas fez sairmos da era do terabyte para o petabyte. Em 2015, entramos na era do zetabytes, e atualmente geramos mais de 2,5 quintilhões de bytes diariamente. O termo *Big Data* surgiu em 1997 e seu uso foi utilizado para nomear essa quantidade cada vez mais crescente e não estruturada de dados sendo gerados a cada segundo. Atualmente o *big data* é essencial nas relações econômicas e sociais e representou uma evolução nos sistemas de negócio e na ciência. As ferramentas de *big data* são de grande importância na definição de estratégias de marketing, aumentar a produtividade, reduzir custos e tomar decisões mais inteligentes. A essência do conceito está em gerar **valor** para negócios. No que tange a ciência, o surgimento do *big data* representou a criação de um novo paradigma (4° paradigma) sendo concebido um novo método de avançar as fronteiras do conhecimento, por meio de novas tecnologias para coletar, manipular, analisar e exibir dados, construindo valor agregado com as análises geradas. BIG DATA. *In:* WIKIPÉDIA. Wikimedia Foundation. 2020. Disponível em: https://pt.wikipedia.org/wiki/Big_data. Acesso em: 04 out. 2023 (grifo nosso).

de Dados, mecanismo de direito comunitário, com vistas a assegurar um conjunto mais robusto e harmônico de regras no âmbito da União Europeia, para a proteção desse direito fundamental. A garantia de uma maior proteção para os indivíduos era essencial também para gerar confiança no ambiente online, tornando possível o desenvolvimento da economia digital através do mercado interno.

O considerando 7 do RGPD[19] discorre sobre esse cenário:

> Esta evolução exige um quadro de proteção de dados sólido e mais coerente na União, apoiado por uma aplicação rigorosa das regras, pois é importante gerar a confiança necessária ao desenvolvimento da economia digital no conjunto do mercado interno. As pessoas singulares deverão poder controlar a utilização que é feita dos seus dados pessoais. Deverá ser reforçada a segurança jurídica e a segurança prática para as pessoas singulares, os operadores económicos e as autoridades públicas.

A principal diferença entre uma diretiva e um regulamento é que este se torna automaticamente aplicável a todos os Estados-membros, não sendo necessário nenhum processo de transposição para a legislação nacional do país, o que garante uma maior coerência na aplicação da lei em toda a União Europeia, superando os problemas ocasionados pelas inconsistências na aplicação das diversas legislações nacionais.

A discussão em torno da proposta do Regulamento ocorreu através de um processo de negociação denominado de trílogo[20] envolvendo a Comissão Europeia,

---

[19] Texto do Considerando 7 do Regulamento Geral de Proteção de Dados. PARLAMENTO EUROPEU. *Regulamento (UE) 2016/679 Do Parlamento Europeu e do Conselho de 27 de abril de 2016*. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 04 out. 2023.

[20] As negociações interinstitucionais tornaram-se uma prática corrente para a adoção da legislação da UE e permitem que os colegisladores cheguem a acordo em qualquer fase do processo legislativo. As negociações entre as instituições sobre propostas legislativas assumem geralmente a forma de reuniões tripartidas (trílogos) entre o Parlamento, o Conselho e a Comissão com o objetivo de chegar a um acordo provisório sobre um texto aceitável tanto para o Conselho como para o Parlamento. Os participantes nos trílogos funcionam com base em mandatos de negociação que lhes são conferidos pelas respectivas instituições. Qualquer acordo provisório alcançado em trílogos é informal e, por conseguinte, tem de ser aprovado pelos procedimentos formais aplicáveis em cada uma das duas instituições. Durante as reuniões do trílogo, que são presididas pelo co-legislador anfitrião da reunião (ou seja, o Parlamento ou o Conselho), as duas instituições explicam a sua posição e desenvolve-se um debate. A Comissão Europeia atua como mediador com vista a facilitar um acordo entre os

o Parlamento Europeu e o Conselho da União Europeia, que resultou, após anos de intensos debates, no Regulamento Geral de Proteção de Dados (RGPD) que entrou em vigor em 24 de abril de 2016, com eficácia plena em 25 de maio de 2018, data em que a Diretiva 95/46 foi revogada.

Vale ressaltar que muito embora o Regulamento vincule automaticamente todos os Estados -membros quanto a sua aplicação, ele permite um certo grau de liberdade no que tange a elaboração de regras mais especificas. É possível, portanto, que haja alguma divergência na aplicação da lei, contudo em um nível muito menor do que o permitido pela legislação anterior. As situações em que a lei permite aos Estados-membros o estabelecimento de disposições nacionais para especificar a aplicação das regras do Regulamento estão descritas no Considerando 10[21]:

> (i) existência de leis setoriais em domínios que necessitam de disposições mais específicas;
> (ii) tratamento de categorias especiais de dados (dados sensíveis);
> (iii) tratamento de dados para o cumprimento de obrigação jurídica, exercício de funções de interesse público ou exercício da autoridade pública de que está investido o responsável pelo tratamento.

Nessa senda, percebe-se que o Regulamento não excluiu o direito dos Estados-membros definirem as situações específicas de tratamento, inclusive a determinação mais precisa de condições em que é lícito o tratamento dos dados pessoais.

---

colegisladores. Disponível em: https://www.europarl.europa.eu/olp/en/interinstitutional-negotiations. Acesso em: 04 out. 2023.

[21] Texto do Considerando 10 do RGPD: "(...) No que diz respeito ao tratamento de dados pessoais para cumprimento de uma obrigação jurídica, para o exercício de funções de interesse público ou o exercício da autoridade pública de que está investido o responsável pelo tratamento, os Estados-Membros deverão poder manter ou aprovar disposições nacionais para especificar a aplicação das regras do presente regulamento. Em conjugação com a legislação geral e horizontal sobre proteção de dados que dá aplicação à Diretiva 95/46/CE, os Estados-Membros dispõem de várias leis setoriais em domínios que necessitam de disposições mais específicas. O presente regulamento também dá aos Estados-Membros margem de manobra para especificarem as suas regras, inclusive em matéria de tratamento de categorias especiais de dados pessoais («dados sensíveis»). Nessa medida, o presente regulamento não exclui o direito dos Estados-Membros que define as circunstâncias de situações específicas de tratamento, incluindo a determinação mais precisa das condições em que é lícito o tratamento de dados pessoais." Disponível em: https://gdpr-text.com/pt/read/recital-10/. Acesso em: 05 out. 2023.

É inegável que o Regulamento trouxe uma ampliação e um fortalecimento dos princípios e regras de proteção de dados, já existentes. Dentre as principais mudanças ocasionadas pela aprovação do Regulamento, cita-se:

> (i) o empoderamento dos indivíduos no ambiente on-line através do fortalecimento dos seus direitos;
> (ii) a necessidade de considerar a proteção de dados no desenvolvimento de novas tecnologias, ao prever a proteção de dados por desenho e por padrão (*privacy by design e privacy by default);*
> (iii) a previsão do princípio da *accountability* que atribui responsabilidade a toda a cadeia de agentes de tratamento, públicos ou privados, que devem ter condições de demonstrar o cumprimento da legislação;
> (iv) a necessidade de, em determinadas situações, indicar um encarregado pelo tratamento de dados (*Data Protection Officer*- DPO),
> (v) o fortalecimento da atuação das autoridades supervisoras de proteção de dados e a previsão do *one stop-shop*[22];
> (vi) a aplicação extraterritorial da legislação

Em suma, o RGPD é bem mais abrangente que a Diretiva, que possuía 34 artigos, ao passo que o Regulamento conta uma parte inicial de exposição de motivos contendo 173 considerandos, além de 99 artigos, que visam a proteção dos direitos e garantias fundamentais dos indivíduos, sem jamais impedir o progresso econômico e social, a consolidação e a convergência das economias no mercado interno.

---

[22] O mecanismo de *One Stop Shop* ou balcão único possibilita que nos casos em que uma organização realize atividade de tratamento de dados em vários Estados-Membros, as autoridades de proteção de dados dos vários países possam atuar de forma cooperada a fim de assegurar uma aplicação uniforme do Regulamento. Esse mecanismo permite às organizações, que possuam sede na UE e realizam atividade transfronteiriça de dados, lidar apenas com uma única autoridade supervisora, definida como a principal, que corresponde a autoridade do local onde se encontre o principal estabelecimento da organização. O Regulamento estabelece que autoridade supervisora principal deve trabalhar de forma cooperada com as demais autoridades envolvidas (autoridades interessadas). Esse mecanismo visa alcançar uma coerência nas decisões e na própria atuação das autoridades e empodera os titulares de dados, na medida em que eles podem reclamar seus direitos perante a autoridade nacional de seu país, mesmo que envolva tratamento transfronteiriço de dados.

O Regulamento Europeu é hoje a legislação mais robusta de proteção de dados existente no mundo e, inclusive, em decorrência de suas regras sobre o fluxo transfronteiriço de dados para países terceiros, tem impulsionado um movimento regulatório a nível global.

7 A INFLUÊNCIA DO SISTEMA EUROPEU DE PROTEÇÃO DE DADOS NA LEGISLAÇÃO BRASILEIRA E SUA RELEVÂNCIA NORMATIVA NO CONTEXTO REGULATORIO MUNDIAL

Com a sanção da Lei 13.709 (Lei Geral de Proteção de Dados – LGPD),[23] em 14 de agosto de 2018, o Brasil ingressou no rol de mais de uma centena de países com legislações gerais de proteção e dados. De modo geral, pode-se afirmar que há uma alta convergência regulatória em proteção de dados, ao redor do mundo. Isso decorre do fato de que a maioria das legislações foram estruturadas sobre as mesmas bases principiológicas, tendo, como parâmetro regulatório, no âmbito europeu, a Convenção 108, primeiro instrumento internacional vinculativo sobre proteção de dados, de 1981, modernizada em 2018.

A necessidade de inserção em uma economia cada vez mais digital e globalizada e o desejo de figurar no mapa global do livre fluxo de dados, tem impulsionado os países a adotarem legislações de proteção de dados com vistas a garantir um nível adequado de proteção aos indivíduos diante do tratamento de seus dados. Sem dúvida, os padrões elevados para as transferências internacionais de dados para os países terceiros, impostos pelo RGPD, têm um papel fundamental nesse movimento regulatório, uma vez que nenhum país deseja ser excluído de um mercado tão importante como o do espaço econômico europeu.

No Brasil, os debates que antecederam a sanção da LGPD duraram quase uma década. A eficácia plena do Regulamento Europeu, que ocorreu em 25 de maio de 2018, é considerada como um dos principais fatores para a aceleração dos debates

---

[23] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em 30 jul. 2023..

legislativos, que culminaram com uma aprovação unânime pelo Congresso, seguida da sanção presidencial, ocorrida em agosto do mesmo ano.

Ao analisarmos as duas legislações, é perceptível a semelhança entre elas, sendo inegável a grande influência do RGPD na lei brasileira. Contudo, importa compreender que o Regulamento Europeu é produto de décadas de evolução legislativa nessa temática pela União Europeia, tendo sido concebido tomando como base a Diretiva 95/46, que vigorou por mais de 20 anos, e com a proteção de dados reconhecida como direito fundamental, pela Carta de Direitos Fundamentais da UE. Nota-se que tanto pela quantidade de artigos, que é maior, quanto pela existência de uma parte introdutória com uma exposição de motivos, que o RGPD é mais robusto e completo, se comparado com a LGPD, que, diferentemente da lei europeia, é a primeira legislação geral sobre a temática no Brasil, tendo sido concebida em momento anterior ao reconhecimento da proteção de dados como um direito fundamental, o que somente ocorreu em fevereiro de 2022, com a promulgação da Emenda Constitucional 115.[24]

Há uma convergência bastante significativa entre os princípios do Regulamento Geral de Proteção de Dados da União Europeia (RGPD) e os princípios da LGPD, em função tanto da forte influência do sistema europeu de proteção de dados na lei do Brasil, como de uma forte harmonização da base principiológica que orienta essa temática ao redor do mundo.

Nessa senda, a LGPD, ao dispor sobre os princípios de proteção de dados, importou os princípios previstos no RGPD e acrescentou três novos: segurança, prevenção e não discriminação, além de incluir o princípio da boa-fé no caput do seu artigo 6º. Esses princípios devem sempre orientar a intepretação e aplicação da lei nas situações concretas, e enfrentar problemas atuais como, por exemplo, o potencial discriminatório do uso de dados nas decisões algorítmicas, o que, em ocorrendo, estará em desconformidade com a lei que, pelo princípio da não discriminação, proíbe o uso de dados pessoais com fins discriminatórios ilícitos ou abusivos.

---

[24] BRASIL. Emenda Constitucional 115, de 10 de fevereiro de 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 05 out. 2023.

De igual modo, é perceptível a similaridade dos direitos dos titulares previstos na LGPD em relação ao RGPD, com pequenas diferenças normativas como no direito ao esquecimento, não previsto na lei brasileira, e nas decisões automatizadas, em que o texto normativo brasileiro não garante a revisão humana, diferentemente da expressa previsão contida na legislação europeia.

Do ponto de vista da licitude das atividades de tratamento, ambas as leis estabelecem em rol taxativo as hipóteses que legitimam o tratamento de dados, as chamadas bases legais, tanto para os dados sensíveis como para os não sensíveis, o que nos permite caracterizar essas legislações como modelos *ex-ante* de proteção.

Os modelos ex-ante de proteção se fundamentam na compreensão de que em uma sociedade da informação, não existem dados irrelevantes. Os dados pessoais, qualquer informação que possa identificar direta ou indiretamente uma pessoa, conceito, portanto, bastante amplo, são verdadeiras projeções de nossas personalidades e merecem proteção, pois o seu uso inadequado tem o condão de gerar riscos para as liberdades e os direitos fundamentais dos titulares de dados.

Um elemento marcante nas legislações mais atuais de proteção de dados, as legislações consideradas de quinta geração, caso do RGPD, que é produto de uma modernização da legislação europeia nessa jornada de empoderamento do titular, e da LGPD, sancionada há apenas 5 anos com forte influência do sistema europeu, é o princípio da *accountability*, que busca atribuir responsabilidade a toda cadeia de agentes de tratamento.

Conforme mencionado em tópico anterior, uma das dificuldades enfrentadas pelas organizações, à época da Diretiva, foi cumprir com os diferentes requisitos para notificação às autoridades supervisoras dos Estados-membros acerca dos tratamentos de dados realizados em cada país.

Atualmente, nem o RGPD e nem a LGPD possuem essa disposição. A legislação europeia determina a comunicação à autoridade supervisora de proteção de dados apenas para os tratamentos que apresentarem um risco elevado para o titular de dados, uma espécie de voto de confiança que é concedido aos agentes de tratamento e que é amparado, em ambas as legislações, por ferramentas através das quais, na lógica da *accountability*, os agentes de tratamento devem demonstrar o

cumprimento da legislação e a eficácia das medidas adotadas para a proteção dos dados pessoais tratados por eles.

Uma dessas ferramentas é o Relatório de Impacto à Proteção de Dados pessoais (RIPD),[25] previsto na LGPD, que embora não seja obrigatório, poderá ser exigido pela Autoridade Nacional de Proteção de Dados (ANPD). Vale ressaltar que este tema se encontra em processo de regulamentação pela ANPD, que deve definir, dentre outras questões, o contéudo e as situações em que ele poderá ser exigido dos agentes de tratamento.

No caso europeu, a ferramenta que desempenha essa função é a Avaliação de Impacto à Proteção de Dados (AIPD) ou, como é mais conhecida, Data Protection Impact Assessment (DPIA). O RGPD apresenta uma lista exemplificativa de situações nas quais os responsáveis pelo tratamento devem elaborar a referida avaliação, e somente quando os riscos residuais ainda forem altos para os titulares de dados, a autoridade supervisora deve ser comunicada.

Além do RIPD ou AIPD, existem outras ferramentas nas respectivas legislações que os agentes de tratamento podem e devem utilizar para comprovar a conformidade com a lei. Desta feita, pode-se afirmar que o princípio da *accountability* garante, por um lado, uma maior flexibilidade e liberdade aos agentes de tratamento no desempenho de suas atividades, mas, por outro lado exige dos mesmos, responsabilidade no cumprimento de seus deveres legais.

Todo esse arranjo normativo mais moderno, pautado no incremento do controle dos titulares sobre seus dados e na atribuição de mais flexibilidade e responsabilidade aos agentes de tratamento no cumprimento de seus deveres legais, visa proteger a personalidade dos indivíduos diante dos riscos que o tratamento de dados pessoais pode lhes ocasionar, fomentando, ao mesmo tempo, o livre fluxo informacional, tão necessário em uma sociedade cada vez mais digital e globalizada.

---

[25] O Artigo 5º, XVII define o relatório de impacto à proteção de dados pessoais como a documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 05 out. 2023.

Por fim, percebe-se uma nítida evolução legislativa do sistema europeu de proteção de dados que acompanhou o desenvolvimento tecnológico e os potenciais riscos decorrentes das novas tecnologias no tratamento de dados pessoais, sempre em busca de uma maior coerência legislativa para o livre fluxo dos dados e na garantia de uma proteção robusta dos titulares, em uma jornada positiva de empoderamento do indíviduo.

REFERÊNCIAS

BIG DATA. *In:* WIKIPÉDIA. Wikimedia Foundation. 2020. Disponível em: https://pt.wikipedia.org/wiki/Big_data. Acesso em: 03 out. 2023.

CONSELHO DA EUROPA. *Convenção para a proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal (Convenção 108) de 28 de janeiro de 1981*. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108. Acesso em: 03 out. 2023.

COUNCIL OF EUROPE. *Convention for the protection of individuals with regard to the processing of personal data (CETS 108). In:–* COE. 2018. Disponível em: https://rm.coe.int/cahdata-convention-108-table-e-april2018/16808ac958. Acesso em: 03 out. 2023.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* Rio de Janeiro: Renovar, 2006.

HORNUNG, Gerrit; SCHNABEL, Christoph. Data Protection in Germany I: the population census decision and the right to informational self-determination. **Computer Law and Security Review,** Kassel, n. 25, p. 84-88, 2009.

MARTINS, Flávio. *Curso de direito constitucional.* São Paulo: Saraiva, 2005.

MENDES, Laura Schertel. *A lei geral de proteção de dados pessoais*: um modelo de aplicação em três níveis. Caderno Especial LGPD. São Paulo: RT**,** 2019**.**

MENKE, Fabiano. Spiros Simitis e a primeira lei de proteção de dados do mundo. **Migalhas,** 19 nov. 2021. Disponível em: http://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/355182/spiros-simitis-e-a-primeira-lei-de-proteçao-de-dados-do-mundo. Acesso em: 03 out. 2023.

PARLAMENTO EUROPEU. *Directiva 95/46/CE do Paralemnto Europeu e do Conselho relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados de 24 de outubro de 1995*.

Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046. Acesso em: 04 out. 2023.

COMISSÃO EUROPEIA. *Relatório Geral sobre a Actividade da União Europeia — 2003 adotado pela Comissão Europeia em 23 de Janeiro de 2004*, p. 109. Disponível em: https://eur-lex.europa.eu/resource.html?uri=cellar:ba77533a-9d00-4687-b77f-a7e598000175.0004.02/DOC_2&format=PDF. Acesso em: 04 out. 2023.

PARLAMENTO EUROPEU. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016*. (Regulamento Geral sobre a Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 04 out. 2023.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais* (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em 30 jul. 2023.

MALDONADO, Viviane Nóbrega. OPICE BLUM, Renato. *Comentários ao GDPR.* 2ª edição. São Paulo: Thompson Reuters Brasil, 2019.

PINHEIRO, Alexandre Sousa. *Comentário ao Regulamento Geral de Proteção de Dados.* Coimbra: Edições Almedina, 2018.

BIONI, Bruno. *Proteção de dados [livro eletônico]: contexto, narrativs e elementos fundantes*. São Paulo: B,R.Bioni Sociedade Individual de Advocacia, 2021.

BRASIL. *Emenda Constitucional 115, de 10 de fevereiro de 2022*. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em 30 jul. 2023. Acesso em: 04 out. 2023.

4. EM DIREÇÃO AO EQUILÍBRIO ENTRE O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS E A UTILIZAÇÃO DA INTELIGÊNCIA ARTIFICIAL NO MUNDO CONTEMPORÂNEO

https://doi.org/10.36592/9786554600798-04

Francisco Soares Campelo Filho[1]

RESUMO
A capacidade mundial de armazenamento de informações praticamente tem dobrado a cada 40 meses desde a década de 1980, projetando-se um aumento de 40% ao ano no volume de dados criados no mundo. Assim, se por um lado os avanços tecnológicos têm trazido inúmeros benefícios à sociedade, por outro têm afetado sobremaneira o direito fundamental à proteção de dados dos indivíduos. Nesse contexto é que emerge a necessidade de que haja um equilíbrio entre o direito fundamental à proteção de dados pessoais e a utilização da inteligência artificial, tanto para que a inteligência artificial possa continuar o seu caminho de evolução em benefício do ser humano e da sociedade, quanto para que o direito fundamental à proteção dos dados possa ser respeitado e efetivado em toda a sua plenitude. O desafio, porém, é como conseguir esse equilíbrio, considerando que os interesses em algum momento se apresentam contrapostos.
Palavras-chave: Direito Fundamental. Proteção de Dados Pessoais. Inteligência Artifical. Constituição. Mundo Contemporâneo.

1. INTRODUÇÃO - A TRANSFORMAÇÃO DIGITAL NO MUNDO CONTEMPORÂNEO: REFLEXOS NO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS

O desenvolvimento da tecnologia, sem dúvida, tem trazido inúmeros benefícios para a humanidade, não só por propiciar desenvolvimento econômico, inclusive com a redução de custos de produção, aumento da produtividade, otimização e automação dos processos, mas também pelos importantes avanços na medicina e na própria educação, contribuindo para a melhoria da qualidade de vida das pessoas. Efetivamente, não há como não se considerar as vantagens obtidas

---

[1] Francisco Soares Campelo Filho é Pós-Doutor em Direito e Novas Tecnologias pela Mediterranea International Centre for Human Rights Research da Università Mediterranea di Reggio Calabria - Itália. Doutor em Direito Público pela UNICEUB (DF). Mestre em Direito Público pela UNISINOS (RS). Membro Consultor da Comissão Especial de Proteção de Dados do Conselho Federal da OAB. Advogado.

pela humanidade através dos avanços tecnológicos, com o uso da inteligência artificial (IA), dos algoritmos, *deep learning*, robôs etc.

Para além desses campos[2], a tecnologia permitiu uma maior integração e interação entre as pessoas, na medida em que possibilitou uma maior conectividade, com troca de conhecimentos e experiências. De fato, a utilização de sistemas com inteligência artificial (IA) e automação (ADM[3]), que permite ainda que objetos se conectem uns aos outros, recebam e enviem informações utilizando a internet, tem sido responsável por um aumento considerável das informações e dos dados que são compartilhados e armazenados em todo o mundo.

A capacidade tecnológica mundial de armazenar, comunicar e computar informações, conforme pesquisa publicada ainda em 2012[4], em que o autor rastreou 60 tecnologias analógicas e digitais durante o período de 1986 a 2007, cresceu a uma taxa anual de 58%, por sua vez a capacidade mundial de telecomunicações bidirecionais cresceu 28% ao ano e as informações armazenadas globalmente tiveram um aumento de 23%.

Segundo a Organização das Nações Unidas – ONU o volume de dados no mundo tem aumentado exponencialmente. Para se ter uma ideia, na matéria intitulada “Big Data for Sustainable Development”, publicada em seu site, a ONU informa que em 2020 foram criados 64,2 zettabytes de dados, o que corresponde a um aumento de 314% em relação a 2015, aduzindo que hoje os dados são coletados passivamente, derivados de interações diárias com produtos ou serviços digitais, incluindo telefones celulares, cartões de crédito e mídias sociais. Ela dá conta ainda de que o volume de dados está crescendo porque estão sendo cada vez mais coletados por dispositivos móveis de detecção de informações e porque a

---

[2] Para uma análise sobre como a inteligência artificial tem transformado a sociedade e os diversos campos onde ela mais tem influenciado ver: KISSINGER, Henry et al. **The Age of A.I. And Our Human Future**. Little, Brown and Company. USA. Boston, MA. 2021. Os autores trazem uma robusta pesquisa sobre o potencial da Inteligência Artificial e seu impacto em várias áreas da atuação do homem, como saúde, economia, geopolítica, além de direito, desenvolvimento urbano, governança e jornalismo, dentre outros.

[3] Sigla em inglês para *Automated decision-making* (ADM).

[4] HILBERT, Martin. **Mapping out the transition toward information societies: social nature, growth, and policies**. University of Southern California. Libraries. Los Angeles, California, 2012. Disponível em https://digitallibrary.usc.edu/asset-management/2A3BF169DD44 Acesso em 18.09.2023

capacidade mundial de armazenar informações praticamente tem dobrado a cada 40 meses, desde a década de 1980.[5]

A utilização de inteligência artificial trouxe também alguns outros aspectos sociais relevantes, bastando observar que essa maior inte(g)ração entre as pessoas, através da expansão da internet e das suas redes de comunicação, aliada à própria globalização econômica, faz com que elas (pessoas), independente do espaço geográfico onde estejam, ou da suas nações originárias, e ainda em face da própria evolução e expansão do conceito de direitos humanos[6], sejam pertencentes a uma única categoria: a de *seres humanos detentores de direitos fundamentais*. A redundância aqui é aparente, e a história assim o confirma, considerando que ao longo da existência humana na terra, muitas atrocidades foram (e ainda são) praticadas contra pessoas justamente por fazerem parte de determinados grupos, religiões, raças ou origens.

Esse conceito de ser humano detentor de direitos fundamentais, sem qualquer adjetivação, possibilita a criação de um sentimento de pertencimento de todos a uma mesma categoria, sem discriminação, preconceitos ou rótulos, estabelecendo uma responsabilidade social para cada um, individualmente, e para todos em conjunto, pelo respeito aos valores sociais ligados à dignidade do ser humano. Não se pode negar que ao longo da história, sem dúvida, houve um continuado avanço em direção a uma socialização global[7], à medida que foram crescendo as discussões e debates sobre a proteção e a defesa dos direitos humanos, onde todos são eticamente e legalmente responsáveis.

Não se pode deixar de reconhecer, assim, a influência da tecnologia e do avanço da utilização da internet e das redes sociais nesse processo que culmina com essa desadjetivação do ser humano e com o surgimento da responsabilização social de todos, individual e coletivamente. Todavia, se por um lado toda essa intensificação das relações entre as pessoas e o aumento exponencial da velocidade

---

[5] Disponível em https://www.un.org/en/global-issues/big-data-for-sustainable-development Acesso em 18.09.2023

[6] TEIXEIRA, Anderson Vinchinkeski. e CAMPELO FILHO, Francisco Soares **A evolução dos direitos humanos sob os influxos dos processos de globalização**. Revista de Direitos Fundamentais e Democracia, Curitiba, v. 16, n. 16, p. 184-199, julho/dezembro de 2014.

[7] BENEYTO, J. Vidal. **Hacia Una Sociedad Civil Global. Desde La Sociedad Mundo**. Madrid. 2003, Taurus.

de informação e de troca de dados permitiu que se pensasse nessa referida categorização, por outro abriu margem para que outros direitos fundamentais fossem violados, como o da proteção de dados, da privacidade e da imagem.

É que os dados se tornaram economicamente valorados, sendo inclusive objeto de comercialização[8], e ainda passaram a ser utilizados de modo que as pessoas começaram a ser manipuladas, a serem dirigidas não de acordo com suas respectivas vontades, mas de acordo com os interesses do mercado ou dos terceiros que possuíam esses dados.

Na referida matéria *The Value of Data*, o Fórum Econômico Mundial apontou que as empresas de plataforma digital e agregadoras de dados capitalizam dados individuais, vendendo para redes de anúncios e profissionais de marketing que buscam atingir segmentos específicos de consumidores, influenciando no comportamento dos compradores e orientando inclusive na dinâmica de fixação de preços dos produtos.

Shoshana Zuboff assinala de forma muito contundente que todo esse processo de utilização dos dados das pessoas que acessam as plataformas digitais dessas empresas, especialmente Google, YouTube e Facebook, tem permitido a criação de uma nova ordem capitalista: o Capitalismo de Vigilância. Nesse sentido, esse novo capitalismo de vigilância já utiliza como objeto negocial, inclusive, o comportamento futuro das pessoas. A autora pontua que se em 2006, as empresas de petróleo e energia dominavam a lista das seis empresas mais valiosas do mundo, o domínio total, hoje, é de empresas de dados e de tecnologia como Google, Apple, Facebook, Amazon e Microsoft.[9]

---

[8] Ver matéria publicada no site do Fórum Econômico Mundial: **The value of data**. Disponível em *https://www.weforum.org/agenda/2017/09/the-value-of-data/* Acesso 18.09.23 A matéria, publicada ainda em 2017, fez referência a estudo da Comissão Europeia, que previa que em 2020 o valor dos dados personalizados chegaria a 1 trilhão de euros, correspondendo a quase 8% do PIB da EU, prevendo ainda que à medida que essa tendência fosse crescendo, haveria um conflito cada vez maior entre o valor dos dados, a privacidade e o consentimento individuais.

[9] "O capitalismo de vigilância reivindica de maneira unilateral a experiência humana como matéria-prima gratuita para a tradução em dados comportamentais. Embora Alguns desses dados sejam aplicados para o aprimoramento de produtos e serviços, o restante é declarado como **superávit** comportamental do proprietário, alimentando avançados processos de fabricação conhecidos como "inteligência de máquina" e manufaturado em produtos de predição que antecipam o que um determinado indivíduo faria agora, daqui a pouco e mais tarde. Por fim, esses produtos de predições são comercializados num novo tipo de mercado para predições comportamentais que chamo de mercados de comportamentos futuros. Os capitalistas de vigilância têm acumulado uma riqueza

Desse modo, tem-se que a utilização dos sistemas de inteligência artificial, utilização de algoritmos e de automação devem necessariamente ser limitados ou fiscalizados para impedir que afetem os direitos fundamentais das pessoas, estes inseridos no campo dos direitos humanos, com respaldo Constitucional nos países democráticos, dentre eles o Brasil, bem como na própria Declaração Universal dos Direitos Humanos.

É inegável que os sistemas de inteligência artificial e de automação podem atentar contra a liberdade das pessoas, o direito à privacidade e proteção de dados, bem como podem servir de instrumento de discriminação, exsurgindo daí a necessidade de que haja uma legislação forte, eficaz juridicamente, focada na proteção desses direitos fundamentais e que não se limite a mitigar os efeitos de eventuais ações que envolvam inovação e tecnologia.

É preciso enxergar os avanços da utilização da inteligência artificial, a despeito de sua grande importância, sob uma ótica que não deixe de ver os direitos fundamentais como essenciais à vida em sociedade em um Estado Democrático de Direito, que por isso mesmo se sobrepõe (ou devem se sobrepor) aos interesses relacionados à utilização desses sistemas de inteligência artificial e de automação, em especial quando estes possam afetar direta ou indiretamente aqueles direitos que são fundamentos intrínsecos à dignidade humana.

2. A PROTEÇÃO DE DADOS COMO UM DIREITO FUNDAMENTAL DO SER HUMANO

Se por um lado se teve (e ainda se tem) todo um benefício pela utilização de sistemas com inteligência artificial e de automação, como já ressaltado na parte introdutória desse artigo, por outro está havendo um abuso da utilização dos dados que são obtidos através da utilização desses referidos sistemas:

> O capitalismo industrial transformava as matérias-primas da natureza em mercadorias, já o capitalismo de vigilância reivindica o material da natureza

---

enorme a partir dessas operações comerciais, uma vez que muitas companhias estão ávidas para apostar no nosso comportamento futuro." ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: A luta por um futuro humano na nova fronteira do poder. Trad. George Schlesinger. Intrínseca, Rio de Janeiro, 2020, pp. 18/19.

> humana para a feitura de uma mercadoria nova. Agora é a natureza humana que é raspada, arrancada e tomada para o projeto de mercado de um novo século. É ofensivo supor que esse dano possa ser reduzido ao fato óbvio de que usuários não recebam pagamento algum pela matéria-prima que fornecem. Essa análise é uma façanha de má orientação usada para institucionalizar um mecanismo de precificação e, portanto, legitimar a extração do comportamento humano para fins de manufatura e venda. Ela ignora o ponto-chave de que a essência da exploração, aqui, é a utilização de nossa vida como dados comportamentais para o aperfeiçoamento do controle de outros sobre nós. [10]

É necessário, pois, que haja uma compatibilização entre o incremento da inovação tecnológica e a utilização dos dados coletados dos indivíduos, mormente por que esses dados estão intrinsecamente ligados aos direitos individuais fundamentais das pessoas, como à intimidade, à privacidade e à liberdade.

Quanto à legislação, a temática da proteção de dados tem sido debatida em diversos países, sobretudo na União Europeia[11]. No Brasil, mas precisamente a partir de 2018, seguindo muito de perto o disposto na *General Data Protection Regulation - GDPR* da União Europeia, foi sancionada a Lei Geral de Proteção de Dados - LGPD, (Lei 13.709/2018) que, após algumas modificações, passou a vigorar a partir de 01 de janeiro de 2021, sendo que as sanções nela estabelecidas entraram em vigor apenas a partir de 01 de agosto de 2021[12].

Não se pode esquecer, todavia, em que pese a necessidade de uma regulação mais forte, que empresas como o Google têm buscado impedir ou limitar a atuação de uma legislação protetiva aos direitos relacionados à proteção de dados. Zuboff assinala que os capitalistas de vigilância são impelidos a lutar por essa *ausência de legislação* com base em uma *lógica que eles mesmos criaram*. Aduz a pesquisadora

---

[10] ZUBOFF, Shoshana. Ob. cit. p. 115.

[11] O regulamento "*General Data Protection Regulation (GDPR)*", que foi aprovado em 2016 na União Europeia, estabelece regras relativas à proteção de pessoas físicas no que diz respeito ao processamento de dados pessoais e regras relativas à livre circulação de dados pessoais, protegendo ainda os direitos e liberdades fundamentais das pessoas naturais e, em particular, o seu direito à proteção de dados pessoais. Ver íntegra do Regulamento em: *https://gdpr-info.eu/art-1-gdpr/*

[12] No Brasil, os debates legislativos em torno da LGPD, passaram pela MP 959/2020, pela Lei 1.179/2020, que deu origem à Lei 14.010/2020, a qual estabeleceu que a LGPD entraria em vigor no dia 01/01/2021 e determinou que os artigos 52, 53 e 54 (que tratam sobre as sanções para quem descumprir a LGPD) entrariam em vigor apenas a partir de 01 de agosto 2021.

que "Google e Facebook colocaram muita pressão para eliminar a proteção privada on-line, limitar regulações, enfraquecer ou bloquear legislações que aumentem a privacidade e impedir qualquer tentava de circunscrever suas práticas porque tais leis são ameaças existenciais ao fluxo desimpedido de superávit comportamental.[13]"

Toda essa preocupação da União Europeia e de outros países democráticos, como o Brasil, relativamente à proteção de dados, significa a grande relevância do direito à proteção de dados para as pessoas e que deveria ser reconhecido como um direito fundamental do ser humano. Nessa perspectiva, ainda em 2009, na obra *Reinventing Data Protection?* [14], os autores afirmaram que o reconhecimento constitucional da proteção de dados como direito fundamental teria um poder transformador e deveria criar a oportunidade para um processo dinâmico, participativo, indutivo e democrático de reinvenção 'em rede' da proteção de dados.

Na Carta dos Direitos Fundamentais da União Europeia[15] de 2012, o artigo 8º reconhece a proteção de dados como um direito fundamental. Todavia, é sabido que ainda há deficiências, tanto doutrinárias quanto jurisprudenciais, sobre a proteção de dados, e por isso mesmo urge que sejam "reconstruídas[16]" para que o direito à proteção de dados possa operar como um direito fundamental pleno ao lado do direito à privacidade, mas independente, e assim poder ser valorado em toda a sua essência.

No caso do Brasil, o reconhecimento do direito à proteção de dados como um direito fundamental ocorreu apenas em 2022, com a Emenda Constitucional

---

[13] ZUBOFF, Shoshana. Ob. cit. pp. 126/127.
[14] GUTWIRTH, Serge. *et al*. **Reinventing Data Protection?** Springer, Dordrecht. Netherlands, 2009.
[15] **CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION**. *Article 8*
Protection of personal data. 1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority. Disponível em *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT* Acesso em 25.09.23
[16] Para a autora, são necessárias duas condições para que o direito à proteção de dados possa operar como um direito fundamental pleno: em primeiro lugar, deve ser reconhecido um «núcleo» ou «essência» do direito à proteção de dados. Em segundo lugar, as violações do direito à proteção de dados devem ser determinadas exclusivamente com base nos próprios princípios pertinentes em matéria de proteção de dados, sem necessidade de recorrer ao direito à privacidade. TZANOU, Maria, **Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right**. International Data Privacy Law, Volume 3, Issue 2, May 2013, Pages 88–99.

115/2022[17], que acrescentou o inciso LXXIX ao seu Art. 5º, assegurando aos cidadãos "o direito à proteção de dados pessoais, inclusive nos meios digitais", os termos do que já estabelecia a Lei Geral de Proteção de Dados – LGPD. Em que pese tardiamente, não deixa de ser um importante avanço, considerando os riscos de danos que podem ser causados às pessoas em face da ausência de uma legislação forte que além de reconhecer esse direito como fundamental, também implemente um sério e eficaz sistema de proteção.

Efetivamente, várias situações podem ser citadas em que o uso dos sistemas de inteligência artificial e de automação é capaz de atentar contra o direito fundamental à proteção de dados. Programas que realizam reconhecimento facial em espaços públicos, por exemplo, podem caracterizar-se como uma espécie de vigilância em massa, da mesma forma que a tecnologia automatizada de reconhecimento de gênero a partir de características faciais, pode terminar por atribuir uma identidade de gênero a alguém que não corresponde à sua verdadeira identidade de gênero.

Um simples sistema de busca pode terminar por desvirtuar o direito à informação ou acesso ao conhecimento, na medida em que pode direcionar as pesquisas que são realizadas, sugestionando o pesquisador para uma determinada linha de raciocínio ou conclusão, ou ainda para algum pensamento ideológico, o que pode afetar o próprio discernimento das pessoas ou mesmo impedi-las de refletirem, de raciocinarem e de construírem suas próprias ideias e tomarem livremente suas decisões.

Outros exemplos poderiam ser dados, como a utilização dos sistemas de inteligência artificial e de automação para aspectos que envolvam a identificação de pessoas condenadas criminalmente, mas que já cumpriram suas penas e estão livres, ou cumprem ainda alguma medida restritiva de direitos, ou que identifiquem o uso de tornozeleiras eletrônicas, ou ainda a utilização de reconhecimento facial para identificação de políticos que respondam processos por supostas práticas de atos de improbidade, enfim. Tais práticas de utilização desses sistemas poderiam sim caracterizar uma forma de constrangimento pessoal, de divulgação de informações

---

[17] CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL (1988).

pessoais e também de discriminação, com possibilidade de causar danos irreparáveis a estas pessoas.

Não se pode esquecer que os sistemas de inteligência artificial e de automação podem atuar de formas imprevisíveis, autonomamente, inclusive reconhecendo pessoas ou gerenciando dados de forma equivocada ou mesmo sujeitos a interferências de outros sistemas e hackers. Por isso que as leis que tratam da proteção de dados precisam tratar com muita profundidade sobre esses direitos individuais fundamentais, inserindo-os com maior relevância de interesse sobre a inovação e o aumento da utilização da inteligência artificial e de tomada de decisão automatizada, exigindo que haja sempre uma análise aprofundada acerca dos eventuais impactos aos direitos fundamentais em face da utilização dos referidos sistemas.

Não se pode esquecer que a tutela dos direitos fundamentais é dever do Estado e está inserido nas constituições democráticas, como no caso do Brasil, por exemplo. Em verdade, no âmbito da Constituição Federal brasileira de 1988, logo em seu art. 1º, III[18], a Dignidade da Pessoa Humana é apontada como princípio fundamental do Estado Democrático de Direito. Inseriu, dessa forma, o legislador constituinte brasileiro, a dignidade humana como fundamento do próprio Estado. Nesse diapasão é que os direitos fundamentais foram também devidamente inseridos no corpo constitucional, sendo corolário daquela própria dignidade da pessoa humana.

Os direitos fundamentais, é preciso ressaltar, possuem dois importantes aspectos, como bem aponta a doutrina. Um é o que corresponde à plena e total eficácia como direitos sociais, já que considerados como *necessidades* iguais a todos, possuindo, portanto, o caráter de universalidade. O outro diz respeito ao fato de que os direitos sociais, onde se inserem os direitos fundamentais, constituem-se em cláusulas pétreas, independente de suas inserções em artigos dispersos do

[18] CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL (1988). Art. 1º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos: (...) III - a dignidade da pessoa humana; (...).

capítulo próprio, considerando-se uma interpretação sistemática do Art. 60, §4°, inciso IV[19], da Constituição Federal de 1988.[20]

Daí exsurge a necessidade de realizar a harmonização entre esses interesses em conflito, direito fundamental à proteção de dados *versus* necessidade de desenvolvimento pela inovação e tecnologia, através de normativos legais, mas sem esquecer que a proteção de dados constitui-se em um direito fundamental do ser humano e que por isso mesmo necessita de amparo integral.

3. A NECESSIDADE DE AMPARO INTEGRAL AO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS

O advento de instrumentos normativos em vários países, especialmente na União Europeia e também na América Latina[21] mostram a preocupação dos países com o direito à proteção de dados, reconhecendo esse direito como um direito fundamental. Todavia, é preciso analisar em que medida esses referidos regramentos efetivamente hierarquizam a proteção de dados das pessoas em relação aos interesses com a inovação e a tecnologia, a fim de que se possa confiar que o direito fundamental à proteção de dados esteja efetivamente protegido em face da utilização de sistemas com inteligência artificial e de automação.

Essa questão acerca da proteção de dados como um direito fundamental e a necessidade de que haja uma regulação mais adequada, que não se baseie unicamente em mitigação dos riscos, já foi trazida de certa forma para discussão no âmbito do Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, oportunidade em que foi realizado estudo onde foi abordada a relação entre aquele Regulamento (GDPR) e a inteligência artificial, considerando-se não só os desafios e oportunidades para indivíduos e sociedade, mas também as formas pelas quais os

---

[19] CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL (1988). Art. 60. A Constituição poderá ser emendada mediante proposta: (...) § 4º Não será objeto de deliberação a proposta de emenda tendente a abolir: (...) IV - os direitos e garantias individuais.

[20] NUNES, Anelise Coelho. Os direitos fundamentais sociais no estado democrático de direito brasileiro: algumas aproximações em torno de seu conteúdo econômico. **Diálogos Constitucionais de Direito Público e Privado**. n. 2. Cap. 2. Porto Alegre: Livraria do Advogado. 2013, pp. 33-43.

[21] Diversos países, além do Brasil, têm legislações de proteção de dados na América Latina, como Chile, Argentina, Uruguai e Colômbia.

riscos poderiam ser combatidos e as oportunidades possibilitadas através do direito e da tecnologia.[22]

Interessante observar que logo no Sumário Executivo, ao referir-se a Inteligência Artificial e "Big Data", os autores do trabalho reconhecem que

> Na última década, a IA passou por um rápido desenvolvimento. Adquiriu uma base científica sólida e produziu muitas aplicações bem-sucedidas. A IA oferece oportunidades de desenvolvimento econômico, social e cultural; sustentabilidade energética; melhores cuidados de saúde; e a difusão do conhecimento. Essas oportunidades são acompanhadas de sérios riscos, incluindo desemprego, desigualdade, discriminação, exclusão social, vigilância e manipulação. (...) A integração da IA e o "Big Data" pode trazer muitos benefícios para o progresso econômico, científico e social. No entanto, também contribui para riscos para os indivíduos e para toda a sociedade, como a vigilância generalizada e influência no comportamento dos cidadãos, polarização e fragmentação na esfera pública.[23]

Nesse diapasão, no referido estudo foram discutidas as tensões e proximidades entre a inteligência artificial e os princípios de proteção de dados, como, em particular, a limitação de finalidade e minimização de dados. Também foi feita uma análise sobre a tomada de decisões automatizadas, considerando até que ponto ela é admissível, as medidas de salvaguarda a serem adotadas e se as pessoas que fornecem seus dados têm direito a explicações individuais. O estudo verificou, assim, que o Regulamento (GDPR) prevê uma abordagem preventiva baseada em riscos, focado na proteção de dados por design e por padrão. Os autores chegam à conclusão de que a inteligência artificial pode ser implementada de forma a estar acorde com a GDPR. Todavia, observou-se que a GPDR não traz orientações

---

[22] SARTOR, Giovanni *et al*.. **The impact of the General Data Protection Regulation (GDPR) on artificial intelligence.** European Parliamentary Research Service Scientific Foresight Unit (STOA), PE 641.530, 2020. O estudo foi conduzido pelo Professor Giovanni Sartor, *European University Institute of Florence*, ante a solicitação do *Panel for the Future of Science and Technology* (STOA) e dirigido pelo *Scientific Foresight Unit*, dentro da *Directorate-General for Parliamentary Research Services* (EPRS) *of the Secretariat of the European Parliament*. O estudo realizado está disponível em *https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf* Acesso em 23.09.23

[23] Idem, p. 2. Tradução livre.

suficientes aos controladores e que suas prescrições precisam ser expandidas e concretizadas. O estudo conclui, ainda, que a abordagem da GDPR está baseada em riscos e que ao invés de conceder direitos individuais, se concentra na criação de uma ecologia sustentável da informação, onde os danos são evitados por medidas organizacionais e tecnológicas.

Verifica-se, assim, que ao invés de focar nos direitos fundamentais, a GDPR teve uma abordagem mais voltada para regular a utilização da inteligência artificial, de modo a colocar a inovação e o aumento da absorção de tecnologia como principal preocupação. Assim, a proteção de direitos fundamentais teria sido tratada de forma secundária, uma vez que a previsão era de que ela só deveria ser realizada até o limite em que a inovação não restasse prejudicada. Nesse sentido, vê-se que a GDPR propõe uma proteção aos direitos tomando por base os riscos da utilização de sistemas com inteligência artificial e automação.

Com o objetivo de promover a absorção da inteligência artificial e, ao mesmo tempo, abordar os riscos associados ao seu uso, a Comissão Europeia produziu um *White Paper on Artificial Intelligence* com opções políticas e regulatórias "para um ecossistema de excelência e confiança". Este documento foi publicado em 19 de fevereiro de 2020, juntamente com uma consulta pública online, com foco em três tópicos distintos: 1. Ações específicas para o apoio, desenvolvimento e absorção da IA em toda a economia e administração pública da UE; 2. Opções para um futuro marco regulatório sobre IA; e 3. Aspectos de segurança e responsabilidade sobre a IA.[24]

Vê-se claramente a preocupação da União Europeia com o desenvolvimento e utilização da Inteligência Artificial, reconhecendo a sua importância, mas também com a necessidade de se trazer maior segurança às pessoas, mormente em face da possibilidade de utilização dos dados de forma a causar sérios danos aos indivíduos e à própria sociedade.

A LGPD no Brasil, apesar de ter tido forte influência da GDPR europeia, logo em seu artigo 1º estabelece que o seu objetivo é *proteger os direitos fundamentais*

---

[24] EUROPEAN COMISSION. **White Paper On Artificial Intelligence - A European approach to excellence and trust**. Brussels, 2020. Disponível em https://commission.europa.eu/system/files/2020-02/commission-white-paper-artificial-intelligence-feb2020_en.pdf Acesso 25.09.23

de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural[25]. Por sua vez, a GDPR em seu artigo 1º estabelece que ela protege *os direitos fundamentais e liberdades das pessoas naturais e, em particular, seus direitos à proteção de dados pessoais*. Há uma sutil diferença entre ambas, posto que a LGPD, a princípio, não traz a proteção de dados como um direito autônomo independente, mas sim atrelado à liberdade e à privacidade, o que poderia caracterizar-se como uma diminuição de seu efetivo valor, considerando, inclusive, tratar-se de um direito fundamental. Provavelmente não quis inovar o legislador, já que à época da promulgação da LGPD não havia o reconhecimento expresso do direito fundamental à proteção de dados, que só veio a ocorrer com o advento da Emenda Constitucional 115/2022, como já se viu.

Destaca-se, porém, que ao tratar dos fundamentos que disciplinam a LGPD, mais especificamente em seu art. 2º, a lei aponta: I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. Percebe-se que a lei aponta vários fundamentos que podem contrapor-se entre si em algum momento. É o caso, por exemplo, do fundamento relacionado ao *desenvolvimento econômico e tecnológico e a inovação* e os fundamentos do *respeito à privacidade* e o da *inviolabilidade da intimidade, da honra e da imagem*.

Se *desenvolvimento econômico e tecnológico e a inovação* são fundamentos da LGPD, da mesma forma que o respeito à privacidade, por exemplo, como podem ser eles compatibilizados de modo a que um não afete ao outro? O respeito à privacidade está inserido como fundamento para mitigar o desenvolvimento econômico e tecnológico? Há incompatibilidade entre um e outro fundamento, considerando que ambos são fundamentos do direito à proteção de dados na LGPD?

---

[25] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965/2014 (Marco Civil da Internet). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Ver íntegra da Lei em *http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm*

Nesse sentir, observa-se que, apesar de toda a legislação existente sobre o direito à proteção de dados, ainda é preciso que haja um maior debate, a fim de que efetivamente esse direito fundamental seja respeitado em toda a sua inteireza, trazendo maior proteção às pessoas nessa relação entre a proteção de dados pessoais e a utilização de sistemas com inteligência artificial e automação.

4. CONCLUSÃO – EM DIREÇÃO AO EQUILÍBRIO ENTRE O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS E A UTILIZAÇÃO DA INTELIGÊNCIA ARTIFICIAL NO MUNDO CONTEMPORÂNEO

Como se viu, faz-se necessário que haja essa compatibilização entre o direito fundamental à proteção de dados pessoais e a utilização da inteligência artificial. O desafio, porém, é como conseguir esse equilíbrio, considerando que os interesses em algum momento se apresentam contrapostos.

Um importante ponto que precisa ser observado é que tudo o que é desenvolvido pelo homem, seja em que seara for, e com o desenvolvimento tecnológico e a utilização de inteligência artificial não deve ser diferente, deve necessariamente ser em benefício do próprio homem, sob pena de desvirtuar-se o propósito da sua existência. Jamais se pode abrir mão dessa humanização do homem e dessa busca por construir sempre uma humanidade mais feliz.

Nesse sentido, o direito fundamental à proteção de dados exsurge como um limite à utilização da inteligência artificial e deve ser pensado como *conditio sine qua non* para o desenvolvimento de qualquer projeto nessa área da tecnologia e da inovação. O que tem ocorrido com a GDPR da União Europeia, conforme apontado acima, onde está mais presente uma abordagem preventiva baseada em riscos, focado na proteção de dados por design e por padrão, deve servir de análise para que uma nova modelagem de proteção possa ser arquitetada, protegendo-se os indivíduos ainda na fase de desenvolvimento desses projetos.

Ademais, não há dúvida que o direito fundamental à proteção de dados pessoais ainda precisa de um maior reconhecimento e uma maior atenção, não apenas porque se trata de direito fundamental, mas também para que haja a sua real efetivação. De nada adianta a existência do comando constitucional se ele não for

efetivamente implementado em toda a sua inteireza na prática social, em respeito à sua própria força normativa.

De fato, a existência de uma Ordem Constitucional expressa uma condição de possibilidade para que a Constituição converta-se "na ordem geral objetiva do complexo de relações da vida", tal como expressa Konrad Hesse ao discorrer sobre a força normativa da Constituição. É que o autor alemão defende que, para que a força normativa de que trata possua eficácia, a Constituição deve transformar-se em uma força ativa, mas para tanto urge que ela seja capaz de "orientar a própria conduta segundo a ordem nela estabelecida" e possa também "identificar a vontade de se concretizar essa ordem", devendo existir não apenas a "vontade de poder", mas também a "vontade de Constituição".[26]

Nesse toar, Hesse aponta que para "um ótimo desenvolvimento da força normativa da Constituição" é preciso que ela seja praticada, não podendo depender tão-só do seu conteúdo. Hesse reconhece, todavia, estar na interpretação da Constituição o ponto nevrálgico para a "consolidação e preservação da força normativa", considerando-se que "a interpretação constitucional está submetida a princípio da ótima concretização da norma (Gebot optimaler Verwirklichung der Norm)", sugerindo que para que haja uma interpretação adequada, faz-se necessário "concretizar de forma excelente, o sentido (Sinn) da proposição normativa dentro das condições reais dominantes numa determinada situação".[27]

Para alcançar esse equilíbrio entre o direito fundamental à proteção de dados pessoais e a utilização da inteligência artificial, pois, faz-se necessário também que haja um amplo debate sobre as aplicações dos sistemas de inteligência artificial e de automação, com vistas a assegurar a efetiva proteção aos dados pessoais, evitando-se ainda a discriminação e estimulando-se a igualdade, mas sem impedir a utilização da inteligência artificial e todo o desenvolvimento tecnológico que traz consigo. Nesse debate, ainda devem participar as autoridades políticas responsáveis pela elaboração das leis, estudiosos das matérias envolvendo direito e tecnologia,

---

[26] HESSE, Konrad. **A Força Normativa da Constituição**. Trad. Gilmar Mendes. Fabris, Porto Alegre. 1991, pp. 18-19.
[27] HESSE. Konrad. Ob. cit. pp. 18-19

bem como os agentes de proteção de dados e controladores de dados, além da própria sociedade.

Por fim, deve ser ressaltado que qualquer que seja a discussão que envolva o direito à proteção de dados, este deve ser analisado sob a ótica de um direito fundamental e que o respeito a este direito é o que trará segurança e confiabilidade para que os dados possam ser armazenados e utilizados adequadamente. Enquanto não houver essa segurança, tampouco poderá afirmar-se que há respeito à própria dignidade da pessoa humana.

REFERÊNCIAS BIBLIOGRÁFICAS

BENEYTO, J. Vidal. **Hacia Una Sociedad Civil Global. Desde La Sociedad Mundo**. Madrid. 2003, Taurus.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965/2014 (Marco Civil da Internet). Diário Oficial da União, Brasília, DF, 15 ago. 2018.

CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION. Disponível em *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT* Acesso em 25.09.23.

CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL (1988).
EUROPEAN COMISSION. **White Paper On Artificial Intelligence - A European approach to excellence and trust**. Brussels, 2020. Disponível em https://commission.europa.eu/system/files/2020-02/commission-white-paper-artificial-intelligence-feb2020_en.pdf Acesso em 25.09.23.

FÓRUM ECONÔMICO MUNDIAL. **The value of data.** Disponível em *https://www.weforum.org/agenda/2017/09/the-value-of-data/* Acesso 18.09.23
GUTWIRTH, Serge. *et al*. **Reinventing Data Protection?** Springer, Dordrecht. Netherlands, 2009.

HESSE, Konrad. **A Força Normativa da Constituição**. Trad. Gilmar Mendes. Fabris, Porto Alegre. 1991.

HILBERT, Martin. **Mapping out the transition toward information societies: social nature, growth, and policies**. University of Southern California. Libraries. Los Angeles, California, 2012. Disponível em https://digitallibrary.usc.edu/asset-management/2A3BF169DD44 Acesso em 18.09.2023.

KISSINGER, Henry et al. **The Age of A.I. And Our Human Future**. Little, Brown and Company. Boston, MA. 2021.

NUNES, Anelise Coelho. Os direitos fundamentais sociais no estado democrático de direito brasileiro: algumas aproximações em torno de seu conteúdo econômico. **Diálogos Constitucionais de Direito Público e Privado**. n. 2. Cap. 2. Porto Alegre: Livraria do Advogado. 2013.

ONU – ORGANIZAÇÃO DAS NAÇOES UNIDAS. **Big Data for Sustainable Development**. Disponível em https://www.un.org/en/global-issues/big-data-for-sustainable-development Acesso em 18.09.2023.

SARTOR, Giovanni *et al*. **The impact of the General Data Protection Regulation (GDPR) on artificial intelligence.** European Parliamentary Research Service Scientific Foresight Unit (STOA), PE 641.530, 2020. Disponível em *https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf* Acesso em 23.09.23.

TEIXEIRA, Anderson Vinchinkeski e CAMPELO FILHO, Francisco Soares **A evolução dos direitos humanos sob os influxos dos processos de globalização**. Revista de Direitos Fundamentais e Democracia, Curitiba, v. 16, n. 16, p. 184-199, julho/dezembro de 2014.

TZANOU, Maria, **Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right**. International Data Privacy Law, Volume 3, Issue 2, May 2013, Pages 88–99.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: A luta por um futuro humano na nova fronteira do poder. Trad. George Schlesinger. Intrínseca, Rio de Janeiro, 2021.

5. NOTAS SOBRE OS LIMITES DO COMPARTILHAMENTO DE DADOS PESSOAIS E A SEPARAÇÃO INFORMACIONAL DE PODERES NO BRASIL – A CONTRIBUIÇÃO DO STF[1]

 https://doi.org/10.36592/9786554600798-05

Ingo Wolfgang Sarlet[2]

Gabrielle Bezerra Sales Sarlet[3]

RESUMO

A concentração crescente de poder informacional, especialmente no que diz respeito aos dados pessoais e os limites de seu compartilhamento, representa um dos maiores desafios para o Estado Democrático de Direito, razão pela qual se tem sustentado a necessidade de reconhecer um princípio e correspondente dever constitucional de separação informacional de poderes. Nesse sentido, o presente texto busca analisar como, no âmbito da ordem jurídica brasileira, a separação informacional de poderes tem sido compreendida e aplicada – direta ou indiretamente – pelo Supremo Tribunal Federal.
Palavras-chave: Compartilhamento de dados pessoais. Separação informacional de poderes. Supremo Tribunal Federal.

1. NOTAS INTRODUTÓRIAS

O princípio-direito-garantia de e a um devido processo informacional tem, no âmbito da evolução das tecnologias de informação e comunicação, da transformação digital e dos fenômenos a ela conexos, assumido um papel cada vez mais central no âmbito do Estado Democrático de Direito, com destaque aqui, dado o foco do presente texto, para a proteção de dados pessoais. Nesse contexto, o

---

[1] O texto ao qual se refere o resumo não será inédito, no sentido de se tratar de reconstrução, atualização e formatação adequada à presente obra coletiva, de texto publicado na forma de artigo científico na Revista Brasileira de Estudos Constitucionais,

[2] Advogado e parecerista. Doutor e Pós-Doutor em Direito pela Universidade de Munique. Professor Titular e Coordenador do Programa de Pós-Graduação em Direito da PUCRS. Desembargador aposentado do TJRS. contato@ingosarlet.com.br

[3] Advogada e parecerista. Mestre em Direito pela UFC. Doutora em Direito pela Universidade de Augsburg. Pós-Doutorado em Direito pela Universidade de Hamburgo e pelo PPGD da PUCRS. Professora Adjunta da Escola de Direito da PUCRS nos níveis de graduação, mestrado e doutorado. Especialista em Neurociências pela PUCRS. gabriellebezerrasales@gmail.com

Estado deve operar também como garante do sigilo, da confiança e da transparência, que, por sua vez, são de capital importância para um devido processo informacional[4].

Outrossim, ainda nessa quadra, é de se sublinhar que o devido processo informacional constitui, de certo modo, uma decorrência lógica e exigência do Estado Democrático de Direito, para além de um mero legado do constitucionalismo liberal, que, em razão da radicalidade das assimetrias, da sutileza, da pervasividade das novas tecnologias e, consequentemente, das possibilidades de práticas abusivas que afetam ou potencialmente podem afetar o processo de tomada de decisão das pessoas (e igualmente dos atores estatais encarregados da proteção e da promoção dos direitos e garantias fundamentais); por isso, o devido processo informacional implica a existência de instrumentos adequados ao estabelecimento de limites aos fatores referidos, como é o caso, e. g., da garantia da ampla defesa e do contraditório, assegurando condições de efetividade reais para o livre desenvolvimento da personalidade, dentre outros direitos e garantias fundamentais[5].

É nesse sentido, que – para ilustrar a questão - se revela imperiosa, em um Estado Democrático de Direito que mereça ostentar essa designação, a vedação de bases de dados comuns, cujo compartilhamento é ilimitado entre e para todos os entes estatais. Dito de outro modo, é crucial que se assegure também uma separação/divisão informacional de poderes, o que se revela ainda mais imperioso e urgente quanto se trata de estabelecer limites ao assim chamado vigilantismo, cada vez mais presente – e mesmo onipresente – também no Brasil, tudo potencializado pelo uso dos recursos da inteligência artificial.

À guisa de ilustração, colaciona-se o pensamento de Byung-Chul no sentido de que o regime de informação consiste em uma forma de dominação na qual os dados ocupam o lugar central, determinando, decisivamente, por meio do emprego de algoritmos e de inteligência artificial, os processos sociais, econômicos e

---

[4] DI FABIO, Udo. *Grundreschtsgeltung in digitalen Systemen*: Selbstbestimmung und Wettbewerb im Netz. München: C.H. Beck, 2016, p. 44-45; V. ainda BIONI, Bruno; MARTINS, Pedro. Devido processo informacional: um salto teórico-dogmático necessário?, Manuscrito. Disponível em: https://brunobioni.com.br/wp-content/uploads/2020/08/Ensaio-Devido-Processo-Informacional1.pdf Acesso em: 02.03.2022

[5] CRAWFORD, Kate; SCHULTZ, Jason. Big data and due process: Toward a framework to redress predictive privacy harms. *BCL Rev*., v. 55, p. 93, 2014. Disponível em: https://lawdigitalcommons.bc.edu/bclr/vol55/iss1/4. Acesso em: 04 mar. 2022.

políticos. Enfatiza-se, nessa perspectiva, que há uma relação direta entre esse regime e o sistema de capitalismo de vigilância no que refere a um exercício de poder voltado para um perfilhamento desproporcional tendo como base uma ação degradante da pessoa humana na medida em que utiliza os dados para abusos quanto a um prognóstico cada vez mais preciso de expectativa de comportamento, inclusive psicopolítico[6].

Em rigor, em face da atual conjuntura tecnopolítica e da ideia de que não existem dados irrelevantes, a proteção de dados pessoais e, consequentemente, a efetividade da autodeterminação informativa, implica a contenção/vedação de unidades/blocos informacionais, privados e públicos que, agindo de forma monolítica, mediante a consequente vitrificação do ser humano, manifestam potencial de intensa lesividade[7] à dignidade da pessoa humana e aos direitos e às garantias fundamentais, sem prejuízo de colocar em cheque a concretização das exigências do Estado Democrático de Direito e de seus princípios estruturantes, o que, por sua vez, implica uma releitura da principiologia constitucional[8].

Por certo, em razão dessa conjuntura, há de se proceder a uma releitura dos cânones constitucionalmente assegurados na ordem jurídica nacional[9], em especial no que diz com a posição da pessoa humana na sociedade informacional, às

---

[6] HAN, Byung-Chul. Infocracia: digitalização e a crise da democracia. Tradução: Gabriel S. Philipson. Petrópoilis, RJ: Vozes, 2022, p. 07. O autor faz uma espécie de comparação entre o regime disciplinar e o regime de informação para afirmar que o capitalismo da informação, assentado sobre a comunicação e a conexão, tornou obsoletas as técnicas disciplinares de isolamento espacial, bem como a rigidez na regulamentação do trabalho e ou o adestramento corporal. Ainda aduz que a natureza da submissão, nesse caso, é distinta, vez que se pressupõe que o sujeito se perceba como livre, autêntico, criativo e performático.

[7] ZUBOFF, Shoshana. *A era do capitalismo de vigilância*: a luta por um futuro humano na nova fronteira do poder. Tradução: George Schlesinger. Rio de Janeiro: Intrinseca, 2020, p. 153-154.

[8] https://www.conjur.com.br/2022-mar-07/polido-ingresso-brasil-ocde-padroes-conformidade Acesso em 26.08.2022 Segundo o autor, "Membros da OCDE, como na pretendida acessão do Estado brasileiro à organização, devem assegurar que padrões adequados de privacidade de dados estejam comprovados tecnicamente, com leis e regulamentos que estabelecem regras relativas às garantias de segurança e confiança de usuários de internet e consumidores digitais, especialmente jovens, além do combate à desinformação e promoção de princípios democráticos e dos direitos humanos associados às operações digitais."

[9] MENDES, Gilmar Ferreira; BRANCO, Paulo Gonet. *Curso de Direito Constitucional*. 15. ed. São Paulo: Saraiva Educação, 2020, p. 126-127.

vulnerabilidades daí decorrentes [10] e às novas formas de proteção como um irrenunciável ponto de partida[11].

Parte-se, ainda, de uma flexibilidade interpretativa dos dispositivos constitucionais admitindo, inclusive, uma interpretação pelo prisma do assim chamado constitucionalismo digital[12] que implica reconfigurações do Estado e do próprio federalismo brasileiro. Além disso, em virtude do papel dos agentes estatais sobretudo a partir da promulgação da EC 115, que incluiu o direito à proteção de dados pessoais no catálogo constitucional, assume ainda maior relevo o dever constitucionalmente vinculativo de desenvolver uma gestão republicana, ética, confiável e segura dos dados durante todo o seu ciclo de vida. Portanto, forjando balizas para algumas condições para o exercício da cidadania digital, intenta-se buscar um discurso factível para o fortalecimento das instituições democráticas e do Estado de Direito[13].

Nesse contexto, evidencia-se, assim, a urgência de uma análise da questão posta à luz da teoria dos direitos fundamentais, e, mais especificamente, com base no princípio da dignidade da pessoa humana, (também) tendo em vista os esforços do Brasil de ascender à condição de legítimo Estado Constitucional Democrático e de Direito Digital, incluindo as providências relativas à edificação de barreiras eficazes contra a formação de uma unidade (e centralização sem limites e controle) informacional, principalmente no que se refere ao compartilhamento irrestrito de

---

[10] MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação algorítmica: conceito, fundamento legal e tipologia. *Direito Público*, Porto Alegre; Brasília, n. 90, nov./dez. 2019, p. 42-43.

[11] RODOTÁ, Stefano. A vida na sociedade da vigilância. Rio de Janeiro: Renovar, 2008, p. 113; SOLOVE, Daniel J. La persona digital y el futuro de la intimidad. *In*: POULLET, Yves; ASINARI, Maria Verônica Pérez; PALAZZI, Pablo (Coord.). *Derecho a la intimidad y a la protección de datos personales*. Buenos Aires: Heliasta, 2009.

[12] ROBL FILHO, Ilton Norberto. Alguns apontamentos sobre o constitucionalismo digital. Revista Consultor Jurídico, 22 de janeiro de 2022. Disponível em: https://www.conjur.com.br/2022-jan-22/observatorio-constitucional-alguns-apontamentos-constitucionalismo-digital. Acesso em: 26.02.2022. Para o autor, "O constitucionalismo digital não se resume às descrições sobre o impacto da tecnologia digital nas relações sociais, jurídicas e constitucionais, assim como não se restringe apenas às prescrições acerca da regulação das tecnologias. O constitucionalismo digital produz uma revisão crítica sobre a estrutura do constitucionalismo". Sobre o tema, v., ainda, o excelente texto de MENDES, Gilmar Ferreira; OLIVEIRA FERNANDES, Victor. Constitucionalismo digital e jurisdição constitucional: uma agenda de pesquisa para o caso brasileiro. *Revista Brasileira de Direito*, Passo Fundo, v. 16, n. 1, p. 1-33, out. 2020. ISSN 2238-0604. Disponível em: https://doi.org/10.18256/2238-0604.2020.v16i1.4103. Acesso em: 28 fev. 2022.

[13] OCDE. Good practice principles for Data Ethics in the Public Sector, 2020, p. 04. Disponível em: www.ocde.org/digital/digital-goverment/good-practice-principles-for-data-ethics-in-the-public-sector.htm Acesso em: 26 fev. 2022.

dados pessoais, ao arrepio das exigências do direito fundamental à proteção de dados e do teor da LGPD, assim como em desconsideração às recomendações da ANPD, mais especificamente, de seu guia orientativo[14] para o tratamento de dados pessoais pelo poder público.

Como já adiantado, o problema da concentração de poder informacional e de uma ausência de limites ao compartilhamento de dados pessoais, não apenas coloca em grave risco a efetividade de um direito fundamental à proteção de dados, mas também a própria ordem democrática e o Estado de Direito.

No caso brasileiro, a partir do reconhecimento de um direito fundamental implicitamente positivado deduzido pelo STF a partir de um conjunto de princípios e direitos fundamentais, mediante decisão de mérito proferida na ADI 6387, em maio de 2020, da relatoria da Ministra Rosa Weber (caso que também já envolvia querela em torno da legitimidade do compartilhamento de dados) tanto a academia jurídica, mas também o STF, passaram a se ocupar cada vez mais da temática, assegurando já alguns avanços significativos, ainda que se esteja relativamente distante de um adequado equacionamento da matéria, o que, aliás, não surpreende, levando em conta o pouco tempo decorrido da decisão acima referida, da entrada em vigor da Lei Geral de Proteção de Dados – LGPD, ademais da inserção, pela igualmente já citada EC 115/22, de um direito fundamental à proteção de dados pessoais no texto da CF.

À vista dessas sumárias considerações, o que se pretende nesse texto, é esboçar algumas linhas a respeito do necessário reconhecimento de um princípio e correspondente dever de separação informacional de poderes na ordem jurídico-constitucional brasileira, designadamente no concernente ao problema do compartilhamento de dados pessoais entre órgãos do poder público, com destaque para o papel assumido pelo STF relativamente ao tema.

[14] ANPD. Tratamento de dados pessoais pelo poder público. Guia orientativo. Versão 1.0. janeiro 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 28.02.2022

2. DA SEPARAÇÃO INFORMACIONAL DE PODERES E DOS LIMITES AO COMPARTILHAMENTO DE DADOS

Tendo em vista o reconhecimento amplo de direitos fundamentais como um dos pontos nucleares de um Estado Constitucional e, já desde o paradigma liberal, a função das Constituições no sentido de estabelecer limites para o exercício do poder político, a condição básica para esse exercício é, como já consolidado no constitucionalismo democrático, a divisão de poderes e de funções entre os órgãos estatais, garantindo-lhes um razoável grau de autonomia, ao mesmo tempo em que se limita os respectivos poderes, mediante sua descentralização e estabelecimento de controles recíprocos[15].

Na precisa descrição de Konrad Hesse, mediante a divisão de poderes são criadas funções e órgãos estatais, que, por sua vez, devem levar a efeito tais funções nos limites de suas respectivas competências constitucionalmente estabelecidas e mediante regras de procedimento vinculativas e suficientemente claras; de todo modo, em rigor, cuida-se de uma distribuição e/ou divisão entre as funções típicas do poder estatal, visto que o poder do Estado como tal é uno e indivisível, assim como é una e indivisível a soberania[16].

Por outro lado, tal como ocorreu com o próprio Estado de Direito e suas demais manifestações (princípios e/ou elementos), também o princípio da divisão de poderes, a despeito de importantes aspectos em comum, não foi objeto de idêntica recepção e concretização em cada ordem jurídico-constitucional, devendo, portanto, ser apresentado e analisado no devido contexto de cada Estado Democrático de Direito, o que, já na origem do Estado Constitucional, pode ser aferido considerando as distinções entre a tradição francesa (mais fiel a um modelo de separação forte e estrita) e a tradição norte-americana, que preferiu edificar e aperfeiçoar um sistema conhecido como de "freios e contrapesos" (*checks and balances*).

De qualquer sorte, ressalvadas as experiências isoladas divergentes (como se deu no Brasil imperial, mediante a previsão de um quarto poder, o assim chamado

---

[15] SILVA, Virgilio Afonso da. Direito Constitucional Brasileiro. São Paulo: Editora da Universidade de São Paulo, 2021, p. 33.
[16] HESSE, Konrad. *Grundzüge des Verfassungsrecht der Bundesrepublik Deutschland*. 20 ed. Heidelberg: C.F. Müller, 1995, p. 28.

Poder Moderador), em regra até segue atual o sistema clássico protagonizado por Montesquieu de uma divisão horizontal de poderes (de desconcentração e recíproca limitação funcional entre órgãos estatais) entre os poderes (funções) legislativo, executivo e judiciário, cuja horizontalidade decorre da circunstância de inexistir qualquer hierarquia entre os respectivos órgãos e funções do poder estatal, todos operando na esfera de suas competências constitucionalmente estabelecidas.

No caso brasileiro, especialmente desde a primeira Constituição da República (1891), mas de modo especialmente estruturado na atual Constituição Federal, o sistema de divisão (chamado pelo constituinte de separação!) de poderes, fortemente inspirado pela tradição norte-americana e igualmente próximo do modelo adotado pela Lei Fundamental da Alemanha (1949), se identifica pelo fato de que os três poderes (órgãos e funções) estatais se caracterizam por uma atuação conjunta e voltada à consecução dos objetivos constitucionais, atuação que se dá de forma desconcentrada, racional e juridicamente limitada por esferas de competência próprias e mecanismos de controle recíprocos.

Com efeito, o princípio da separação dos poderes tem como objetivo o controle do poder pelo poder, ou seja, mediante um esquema de fiscalização recíproca, que se materializa por um conjunto diferenciado de técnicas e de instrumentos, como é o caso do direito de veto do chefe do Poder Executivo, a própria possibilidade de edição de atos normativos pelo Executivo, a aprovação pelo Legislativo do orçamento dos demais órgãos estatais, o controle judicial dos atos dos demais Poderes, entre outros. Tendo em conta, contudo, a relevância da separação de poderes, o correspondente princípio será objeto de maior desenvolvimento em face da atual digitalização do Estado e de suas estruturas de Governo[17].

Nesse sentido, a separação informacional de poderes da qual ora se trata, consiste em uma ressignificação, tanto lógica, quanto necessária, da semântica do princípio da divisão de poderes (artigo 2º CF) à luz do constitucionalismo digital, tendo em vista, em especial, o problema dos níveis crescentes de poder informacional do Estado brasileiro, bem como da ausência de um regras e critérios

---

[17] Para o caso brasileiro, v. a Lei 14.129/2021, que institui o Governo digital.

que limitam tal concentração e o compartilhamento de dados que a alimenta. Tal estado de coisas, implica, por sua vez, o estabelecimento de uma separação nítida entre as diversas áreas de atuação estatal sob pena de descumprimento de um preceito fundamental e, consequentemente, uma violação das exigências essenciais do Estado Democrático de Direito.

Na condição – aqui advogada – de princípio fundamental estruturante, implicitamente positivado pela CF, a separação/divisão informacional de poderes vincula toda a atuação do Estado brasileiro, como norma de eficácia direta e que, dentre outros requisitos, deve ser concretizado pelo legislador e exige a motivação das decisões que envolvam todas as formas de tratamento de dados, sobretudo dados pessoais, para a configuração efetiva de uma proteção multinível[18] da pessoa humana na sociedade informacional, o que guarda sinergia com o que se extrai das recentes decisões em sede de controle de constitucionalidade exaradas pelo STF, justamente quando em causa os limites do compartilhamento de dados pessoais entre órgãos do poder público.

Num primeiro importante julgamento, o da ADI 6529, ocorrido em 08.10.2021, a relatora, Ministra Cármen Lúcia, consignou que "a Constituição da República repudia poder sem controle, exige a motivação dos atos administrativos e que todos eles se guiem pelos princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência. As atividades de inteligência, ainda que acobertadas pelo sigilo, se submetem ao escrutínio externo dos demais Poderes (Legislativo e Judiciário), devendo ser afastada qualquer interpretação que dê margem a arbitrariedades".

No mesmo julgado, tomando como referência o caso do compartilhamento de dados pelo SISBIN- Sistema Brasileiro de Inteligência com a ABIN- Agência Brasileira de Inteligência, o STF, por unanimidade, decidiu que:

[18] TRIBUNAL decide que Sistema de Indicação de Risco viola direitos humanos. InternetLab, 2020. Disponível em: https://internetlab.org.br/pt/itens-semanario/holanda-tribunal-decide-que-sistema-de-indicacao-de-risco-viola-direitos-humanos/. Acesso em:11 mar. 2022. O Tribunal Distrital de Haia concluiu que o uso do SyRI não encontrou um equilíbrio entre o direito à privacidade e o interesse público em detectar fraudes, indo contra o estabelecido no artigo 8º da Convenção Europeia de Direitos Humanos (CEDH), que prevê o direito à vida privada.

> (i) Os órgãos componentes do Sistema Brasileiro de Inteligência somente podem fornecer dados e conhecimentos específicos à Abin quando comprovado o interesse público da medida, afastada qualquer possibilidade de o fornecimento desses dados atender a interesses pessoais ou privados;
> (ii) Toda e qualquer decisão de fornecimento desses dados deverá ser devida e formalmente motivada para eventual controle de legalidade pelo Poder Judiciário;
> (iii) Mesmo quando presente o interesse público, os dados referentes às comunicações telefônicas ou dados sujeitos à reserva de jurisdição não podem ser compartilhados na forma do dispositivo, em razão daquela limitação, decorrente do respeito aos direitos fundamentais;
> (iv) Nas hipóteses cabíveis de fornecimento de informações e dados à Abin, são imprescindíveis procedimento formalmente instaurado e a existência de sistemas eletrônicos de segurança e registro de acesso, inclusive para efeito de responsabilização em caso de eventual omissão, desvio ou abuso.

Igualmente digna de nota é a decisão monocrática proferida pelo Ministro Gilmar Mendes em sede cautelar, na ADPF 695-DF, que versa sobre o compartilhamento de dados pessoais pelo Serviço Federal de processamento de Dados (SERPRO) com a Agência Brasileira de Inteligência (ABIN), com suposto lastro normativo no Decreto nº. 10.046, que revogou o Decreto 8.789/19, passando a disciplinar o compartilhamento de dados no âmbito da Administração Pública Federal, ademais de instituir o Cadastro Base do Cidadão (CBC) e criar o Comitê Central de Governança de Dados (CCGD). Na sua decisão, o Ministro afirmou que: "o regime jurídico de compartilhamento de dados entre órgãos e instituições do Poder Público é matéria de extrema relevância para a proteção constitucional do direito constitucional à privacidade (artigo 5º, caput e incisos X, da Constituição Federal), situando-se como garantia elementar de qualquer sociedade democrática contemporânea"[19].

[19] STF, ADPF-MC 695. Disponível em: http://portal.stf.jus.br/processos/downloadPeca.aspt=.pdf . Acesso em: 12.03.2022

Recentemente, (15.09.22) em sede de decisão definitiva, o relator das demandas – acompanhado pela maioria dos Ministros, entendeu pelo conhecimento da ADI e da ADPF para, julgando parcialmente procedentes os pedidos, optar por conferir interpretação conforme ao teor do Decreto 10.046/2019.

Evidencia-se que, segundo o Ministro Gilmar Mendes, o compartilhamento de dados passa a ter cada vez uma posição central na atuação do Estado, sobretudo no que se refere às políticas públicas, de tal sorte que pressupõe a conformidade com a LGPD, notadamente do ponto de vista da indicação de propósitos legítimos, específicos, e explícitos para todas as etapas do tratamento. Assim, as finalidades, primárias e secundárias, caso necessário, devem ser devidamente compatibilizadas, vez que o compartilhamento, em si, deve ser restrito ao mínimo e balizados pelo cumprimento dos requisitos, das garantias e dos procedimentos legais.

Extrai-se ainda do voto proferido, que o compartilhamento dos dados pessoais entre os órgãos públicos pressupõe o enquadramento ao que dispõe o artigo 23, I, da LGPD, notadamente quanto à publicidade às hipóteses em que cada entidade governamental compartilha ou tem acesso. Em suma, o entendimento ministerial foi de que o acesso de órgãos e de entidades governamentais ao Cadastro Base do Cidadão fica condicionado ao que outrora foi referido.

Outro ponto que merece destaque diz com as competências do Comitê Central de Governança de Dados, na medida em que, segundo o relator, deveriam ser restringidas/atribuídas às que foram expressas no artigo 21, VI, VII e VIII do Decreto 10.046/2019, desde que atue no estabelecimento e na prevenção de mecanismos rigorosos no controle de acesso ao Cadastro Base do Cidadão. Dito de outro modo, instituiu-se o dever de órgãos e de entidades públicas de demonstrarem a real necessidade de acesso e de compartilhamento. Para tanto, ainda como se extrai do voto, permissão somente deverá ser concedida para o alcance de propósitos legítimos, específicos e explícitos, sendo limitada às informações que sejam indispensáveis ao atendimento do interesse público, nos termos do artigo 7, III, bem como do artigo 23, caput, I da Lei 13.709/2018.

Além disso, estabeleceu-se, para fins de compartilhamento de dados, a obrigação de justificativa prévia e minudente, baseada no emprego da proporcionalidade, da razoabilidade e da principiologia da LGPD, tanto para a

necessidade de inclusão de novos dados pessoais na base integradora quanto no que toca à escolha das bases temáticas do Cadastro Base do Cidadão[20].

O Ministro relator orienta a instituição de medidas de segurança na qualidade de um sistema eletrônico de registro de acesso para efeitos de responsabilização em casos abusivos. Orienta, outrossim, que o compartilhamento nas atividades de inteligência deve seguir os critérios estabelecidos em legislação própria, bem como parametrizados pela decisão do STF no já analisado caso envolvendo a ABIN. Importa destacar a atribuição de reponsabilidade civil do Estado pelos danos suportados aos particulares em consonância com a dicção do artigo 42 e seguintes da LGPD, associando-se o direito de regresso contra os servidores e agentes públicos responsáveis pelo ato ilícito, em caso de culpa ou de dolo.

A decisão, retomando-se aqui, em apertada síntese, os seus elementos centrais, por maioria, entendeu que o compartilhamento de dados pessoais entre os órgãos e as entidades da Administração pública pressupõe: 1- eleição de propósitos legítimos, específicos e explícitos para o tratamento; 2- compatibilidade do tratamento com as finalidades informadas; 3- limitação do compartilhamento ao mínimo necessário para o atendimento da finalidade informada, bem como o cumprimento integral dos requisitos, das garantias e dos procedimentos estabelecidos na LGPD, particularmente no que se refere ao setor público. Restou evidente que essa modalidade de compartilhamento de dados pessoais deve ser publicizado e estar atrelado ao fornecimento de informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, preferencialmente de forma a ser amplamente acompanhada pela população.

Destaque-se, ainda, na decisão, que o acesso ao Cadastro Base do Cidadão por parte de órgãos e de entidades governamentais fica condicionado, para além do que já fora decidido, à atuação do Comitê Central de Governança de Dados. Este, por sua vez, deve: 1- prever mecanismos rigorosos de controle de acesso na medida da comprovação da real necessidade de acesso; 2- observância dos parâmetros da razoabilidade, da proporcionalidade, bem como dos princípios já consagrados na

---

[20] STF, ADI 6649/DF e ADPF 695. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=6079238 Acesso em: 09.10.2022

LGPD para a permissão de acesso que, evidentemente, tem que estar de acordo com o interesse público; 3- indicação das bases temáticas que deverão compor o Cadastro Base do Cidadão; 4- instituição de medidas de segurança compatíveis com o sistema protetivo em vigor no país, sobretudo mediante a criação de sistema eletrônico de registro de acesso com finalidade de aferir a reponsabilidade em casos de abuso.

Oportunamente, deve-se elencar que, seguindo a posição outrora explicitada pelo ministro Gilmar Mendes, o STF decidiu que, em se tratando de atividades de inteligência deve ser seguido o padrão/modelo advindo em legislação específica, bem como os parâmetros fixados no julgamento da ADI 6529. Ainda em conformidade com o voto do relator, restou claro que o tratamento dos dados pessoais promovido por órgãos públicos ao arrepio das balizas, legais e constitucionais, do ordenamento jurídico brasileiro, importará em responsabilidade civil do Estado pelos danos suportados pelos particulares.

Importante reafirmar que quedou decidido que a transgressão dolosa ao dever de publicidade estabelecido no artigo 23, I, da LGPD, fora das hipóteses constitucionais de sigilo, importará a responsabilização do agente estatal por ato de improbidade administrativa. Por derradeiro, com efeito *pro futuro*, o STF declarou a inconstitucionalidade do artigo 22 do Decreto 10.046/19, preservando, no entanto, a atual estrutura do Comitê Central de Governança de Dados pelo prazo de sessenta dias a contar da data da publicação da ata de julgamento. Agrega-se, por outro lado, esse prazo deveria ser adequado para que o Chefe do Executivo atue no sentido de atribuir ao órgão a independência, a autonomia e a pluralidade que são bases inarredáveis para a sua constitucionalidade.

À vista do exposto (ainda que em caráter sumário), tanto a eficácia quanto a efetividade dos direitos fundamentais consagrados na CF, destacando-se aqui o direito à proteção de dados pessoais e a autodeterminação informativa, está diretamente atrelada à consolidação do princípio da separação de poderes (incluída a separação informacional) que, como já se tornou evidente, sofreu mutações consideráveis ao longo dos últimos tempos, especialmente em relação à configuração digital que o Estado brasileiro tem assumido para poder acompanhar a

intensidade das transformações sociais, tecnológicas e tecnopolíticas[21], em um contexto complexo marcado, por um lado, pela hiperconectividade, ao mesmo tempo em que impera, ainda, a divisão digital[22] no Brasil e em grande parte do Mundo.

Quanto a esse ponto, calha lembrar que o artigo 5, X da LGPD clarificou o conceito de tratamento dos dados pessoais, inserindo, dentre outras, as modalidades da coleta, recepção, classificação, utilização, acesso, armazenamento, eliminação, modificação, comunicação e transferência de dados. A LGPD, que aqui concretiza exigências do Estado Democrático de Direito, vincula os agentes estatais (além dos atores privados) como destinatários de suas disposições normativas, inclusive impondo o estabelecimento de programas de governança ética de dados e da previsão de medidas de *accountability*, ademais da produção de uma regulamentação apropriada para a área da segurança em geral e, em particular, daquilo que se tem designado de segurança cibernética[23].

Dentre as searas mais desafiadoras que se tem colocado e exigido reações eficazes com vistas ao enfrentamento dos inúmeros problemas acarretados[24], devem ser mencionadas as que advém a partir do uso de inteligência artificial e na formação e emprego de Big Data[25], vez que colocam em risco os direitos humanos e fundamentais em risco, podendo produzir e acentuar discriminação por meio de generalizações ou de estereotipações e de práticas abusivas de perfilhamento, de análise preditiva e de vigilantismo, acirrando assimetrias informacionais e, em razão

---

[21] HUI, Yuk. *Tecnodiversidade*. Tradução: Humberto do Amaral. São Paulo: Ubu, 2020, p. 39-46.

[22] "Em 2020, a proporção de domicílios com acesso à internet chegou a 83%, o que representa aproximadamente 61,8 milhões de domicílios com algum tipo de conexão à rede", Cf. Disponível em: https://cetic.br/media/docs/publicacoes/2/20211124201505/resumo_executivo_tic_domicilios_2020.pdf . Acesso em: 02 mar. 2022. "Houve aumento na proporção dos usuários que procuraram informações oferecidas por *websites* de governo (de 28% para 42%) e que realizaram algum serviço público pela Internet (de 28% para 37%) (Gráfico 3). No entanto, a realização dessas atividades foi mais frequente, sobretudo, entre aqueles que já realizavam uma variedade maior de atividades na Internet. A realização de serviços públicos *on-line*, por exemplo, foi mais mencionada por usuários da área urbana (39%), de classe A (63%) e por indivíduos com Ensino Superior (68%)."; Cf. NEMER, David. *Tecnologia do oprimido*: desigualdade e o mundano digital nas favelas do Brasil. Vitória: Milfontes, 2021, p. 73-79.

[23] V., a respeito do tema, em caráter ilustrativo, o problema que se está verificando no estado do Ceará, de modo a entender em que consiste um vigilantismo desproporcional (Disponível em: https://direitosnarede.org.br/2020/09/04/nota-sobre-projeto-de-videomonitoramento-no-ceara-e-em-defesa-de-maior-debate-publico/. Acesso em: 12.03. 2022).

[24] WEIDENFELD, Nathalie; NIDA-RÜMELIN, Julian. *Digitaler Humanismus:* Eine Ethik für das Zeitalter der künstlichen Intelligenz. München: Piper, 2018.

[25] HOFFMANN-RIEM, Wolfgang. Big Data e Inteligência Artificial: desafios para o Direito. *REI-Revista Estudos Institucionais*, v. 6, n. 2, p. 431-506, 2020.

disso, violando a esfera da privacidade e a dignidade da pessoa humana[26]. Vem a calhar, nesse contexto, dada a sua atualidade, a lição de Arendt, ao afirmar que “a esfera pública, enquanto mundo comum, reúne-nos na companhia um dos outros e, contudo, evita que colidamos uns com os outros, por assim dizer”[27].

CONSIDERAÇÕES FINAIS

Sabe-se, de há muito, que a coleta e tratamento de dados pelo Estado é, de todo modo, inevitável e mesmo necessária no âmbito do atual cenário de desenvolvimento, inclusive e em especial para que o Estado possa dar conta de suas tarefas, de cada vez mais diversificada, complexa e difícil definição e execução.

Por outro lado, como já anunciado, indispensável o estabelecimento e afirmação de balizas, éticas, técnicas e jurídicas, no que diz respeito à coleta, tratamento, armazenamento, utilização e compartilhamento de dados pessoais, pena de se correr sério risco no sentido da instauração do arbítrio e da erosão dos princípios estruturantes do Estado Democrático de Direito.

Nessa perspectiva, mais do que oportuno colacionar o entendimento de Greco, para quem:

> Se saber é poder, o Estado não pode saber tudo, porque um Estado que tem conhecimentos ilimitados tem também um poder ilimitado. O direito de proteção de dados, que começa como direito subjetivo, mostra-se, ao menos em boa parte, como garantia institucional, relativa à própria estrutura da sociedade e do Estado. ***Nesse nível macro o direito se transforma em uma exigência de separação informacional de poderes***[28] (Grifos nossos).

---

[26] BÄCHLE, Thomas Christian. *Digitales Wissen, Daten und Überwachung: zur Einführung*. Hambug: Junius, 2016, p. 158.

[27] ARENDT, Hannah. A condição humana. Roberto Raposo (trad). Rio de janeiro: Forense, 2001, p. 62.

[28] WOLTER, Jürgen. O inviolável e o intocável no direito processual penal: reflexões sobre dignidade humana, proibições de prova, proteção de dados (e separação informacional de poderes) diante da persecução penal. Luís Greco (tradução, organização e introdução). Eduardo Viana e Alaor Leite (tradução). São Paulo: Marcial Pons, 2018, p. 45.

A proteção de dados implica, dessa forma, a incorporação definitiva de uma cultura pautada pelos princípios e direitos fundamentais (não só, mas em especial o direito à proteção de dados pessoais, a dignidade da pessoa humana e a separação informacional de poderes) e em sinergia com a LGPD, o que deve ser assumido como tarefa pelo Estado brasileiro, que deve estabelecer, mediante a utilização de parâmetros de atuação forjados com base no princípio da separação de poderes, um regime organizacional pautado na divisão por competências, envidando todos os esforços para evitar o compartilhamento abusivo, desproporcional, irrestrito e, portanto, inconstitucional de dados pessoais. Oportuno lembrar que a efetividade do direito fundamental à proteção de dados pessoais é incompatível com medidas que visam ou oportunizem o tratamento indiscriminado de dados pessoais pelos órgãos estatais.

É também por tais razões que o controle com base no parâmetro da finalidade se revela de tamanha importância e consiste em um dos esteios da proteção de dados. Nesse sentido, relembra-se que o controle da atuação do Estado por meio do emprego do critério da finalidade introduz a lógica de que deve ser vedada a atuação do mesmo como uma unidade absoluta, ou seja, de que deve ser assegurada uma divisão de competências constitucionalmente asseguradas (no sentido de uma divisão/separação informacional de poderes), especialmente no que diz respeito ao compartilhamento de dados e seus limites.

Isso, por seu turno, implica o fortalecimento pelo Estado dos níveis de confiança na sua atuação protetiva[29], o que inclui a adoção de medidas que instituam e garantam uma adequada (constitucionalmente conforme) governança de dados, no sentido, dentre outros aspectos, de assegurar a transparência, a prestação de contas e a ampliação da participação popular e do exercício da cidadania.

A implantação de um Estado Democrático Digital de Direito, impende destacar, deve ser voltada para o cidadão, mediante a implementação de um ecossistema inovador e suficientemente seguro, transparente e confiável, que minimize os danos e riscos causados e gerados pelas Tecnologias de Informação e Comunicação e pela Inteligência Artificial (apenas para citar as mais importantes nesse contexto)

[29] Vide, em caráter ilustrativo, o disposto no artigo 2º, I da Lei 13.874/2019, que prevê entre seus princípios, a boa-fé dos particulares perante o poder público.

mediante o recurso a garantias técnicas e jurídicas orientadas pela proteção e promoção da dignidade da pessoa humana, de sua autodeterminação informacional, da proteção de seus dados pessoais e outros direitos e garantias fundamentais, vedando-se qualquer tipo de prática abusiva, inclusive no que diz respeito à segurança cibernética, o que, por sua vez, pressupõe a garantia plena de um devido processo informacional e de uma separação informacional de poderes.

Tendo em conta a evolução recente no Brasil, em especial com base nos julgados acima referidos e discutidos do STF, há razões para otimismo, porquanto a Suprema Corte brasileira tem tido um papel protagonista no processo, não apenas do reconhecimento de um direito fundamental à proteção de dados pessoais antes mesmo de sua inserção no texto da CF, quanto no campo do estabelecimento de limites à concentração de poder informacional, tudo a contribuir também para fortalecer – ou, pelo menos (o que já não é pouco, considerando os tempos atuais) – o Estado Democrático de Direito instituído e formatado pelo Constituinte de 1988.

REFERÊNCIAS

ANPD. **Tratamento de dados pessoais pelo poder público**. Guia orientativo. Versão 1.0. janeiro 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 28.02.2022.

ARENDT, Hannah. ***A condição humana***. Roberto Raposo (trad). Rio de janeiro: Forense, 2001.

ASINARI, Maria Verônica Pérez; PALAZZI, Pablo (Coord.). ***Derecho a la intimidad y a la protección de datos personales*****.** Buenos Aires: Heliasta, 2009.

BÄCHLE, Thomas Christian. ***Digitales Wissen, Daten und Überwachung:*** *zur Einführung*. Hambug: Junius, 2016.

BIONI, Bruno; MARTINS, Pedro. **Devido processo informacional**: um salto teórico-dogmático necessário?, Manuscrito. Disponível em: https://brunobioni.com.br/wp-content/uploads/2020/08/Ensaio-Devido-Processo-Informacional1.pdf Acesso em: 02.03.2022.

CRAWFORD, Kate; SCHULTZ, Jason. **Big data and due process**: Toward a framework to redress predictive privacy harms. *BCL Rev*., v. 55, p. 93, 2014. Disponível em: https://lawdigitalcommons.bc.edu/bclr/vol55/iss1/4. Acesso em: 04 mar. 2022.

DI FABIO, Udo. ***Grundreschtsgeltung in digitalen Systemen***: Selbstbestimmung und Wettbewerb im Netz. München: C.H. Beck, 2016.

ENDES, Laura Schertel; MATTIUZZO, Marcela. **Discriminação algorítmica:** conceito, fundamento legal e tipologia. *Direito Público*, Porto Alegre; Brasília, n. 90, nov./dez. 2019.

HAN, Byung-Chul. **Infocracia**: digitalização e a crise da democracia. Tradução: Gabriel S. Philipson. Petrópoilis, RJ: Vozes, 2022.

HESSE, Konrad. ***Grundzüge des Verfassungsrecht der Bundesrepublik Deutschland***. 20 ed. Heidelberg: C.F. Müller, 1995.

HOFFMANN-RIEM, Wolfgang. **Big Data e Inteligência Artificial:** desafios para o Direito. *REI-Revista Estudos Institucionais*, v. 6, n. 2, p. 431-506, 2020.

HUI, Yuk. ***Tecnodiversidade***. Tradução: Humberto do Amaral. São Paulo: Ubu, 2020.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gonet. ***Curso de Direito Constitucional*.** 15. ed. São Paulo: Saraiva Educação, 2020.

MENDES, Gilmar Ferreira; OLIVEIRA FERNANDES, Victor. **Constitucionalismo digital e jurisdição constitucional**: uma agenda de pesquisa para o caso brasileiro. *Revista Brasileira de Direito*, Passo Fundo, v. 16, n. 1, p. 1-33, out. 2020. ISSN 2238-0604. Disponível em: https://doi.org/10.18256/2238-0604.2020.v16i1.4103. Acesso em: 28 fev. 2022.

NEMER, David. ***Tecnologia do oprimido***: desigualdade e o mundano digital nas favelas do Brasil. Vitória: Milfontes, 2021.

NOTAS sobre projeto de videomonitoramento no Ceará e em defesa de maior debate público. Coalização de Direitos na Rede, 2020. Disponível em: https://direitosnarede.org.br/2020/09/04/nota-sobre-projeto-de-videomonitoramento-no-ceara-e-em-defesa-de-maior-debate-publico/. Acesso em: 12.03. 2022.

OCDE. **Good practice principles for Data Ethics in the Public Sector**, 2020, p. 04. Disponível em: www.ocde.org/digital/digital-goverment/good-practice-principles-for-data-ethics-in-the-public-sector.htm Acesso em: 26 fev. 2022.

POLIDO, Fabricio Bertini Pasquot. **Ingresso do Brasil na OCDE e padrões em matéria digital**. Conjur, 2022. Dispoíbel em: https://www.conjur.com.br/2022-mar-07/polido-ingresso-brasil-ocde-padroes-conformidade. Acesso em 26.08.2022.

RESUMO **Executivo TIC Domicílios 202**0, Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação – CETIC, 2020. Disponível em:

https://cetic.br/media/docs/publicacoes/2/20211124201505/resumo_executivo_tic_domicilios_2020.pdf. Acesso em: 02 mar. 2022.

ROBL FILHO, Ilton Norberto. **Alguns apontamentos sobre o constitucionalismo digital**. Revista Consultor Jurídico, 22 de janeiro de 2022. Disponível em: https://www.conjur.com.br/2022-jan-22/observatorio-constitucional-alguns-apontamentos-constitucionalismo-digital. Acesso em: 26.02.2022.

RODOTÁ, Stefano. A **vida na sociedade da vigilância**. Rio de Janeiro: Renovar, 2008.

SOLOVE, Daniel J. **La persona digital y el futuro de la intimidad**. *In*: POULLET, Yves; SILVA, Virgilio Afonso da. ***Direito Constitucional Brasileiro***. São Paulo: Editora da Universidade de São Paulo, 2021.

STF, **ADI 6649/DF e ADPF 695**. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=6079238 Acesso em: 09.10.2022.

STF, **ADPF-MC 695**. Disponível em: http://portal.stf.jus.br/processos/downloadPeca.asp?id=15343579920&ext=.pdf. Acesso em: 12.03.2022.

TRIBUNAL decide que Sistema de Indicação de Risco viola direitos humanos. InternetLab, 2020. Disponível em: https://internetlab.org.br/pt/itens-semanario/holanda-tribunal-decide-que-sistema-de-indicacao-de-risco-viola-direitos-humanos/. Acesso em:11 mar. 2022.

WEIDENFELD, Nathalie; NIDA-RÜMELIN, Julian. ***Digitaler Humanismus****:* Eine Ethik für das Zeitalter der künstlichen Intelligenz. München: Piper, 2018.

WOLTER, Jürgen. ***O inviolável e o intocável no direito processual penal***: reflexões sobre dignidade humana, proibições de prova, proteção de dados (e separação informacional de poderes) diante da persecução penal. Luís Greco (tradução, organização e introdução). Eduardo Viana e Alaor Leite (tradução). São Paulo: Marcial Pons, 2018.

ZUBOFF, Shoshana. ***A era do capitalismo de vigilância*****:** a luta por um futuro humano na nova fronteira do poder. Tradução: George Schlesinger. Rio de Janeiro: Intrinseca, 2020.

6. COMENTÁRIOS ACERCA DO PARECER DA AUTORIDADE EUROPEIA PARA A PROTEÇÃO DE DADOS REFERENTE AO ACORDO INTERNACIONAL SOBRE O INTERCÂMBIO DE DADOS PESSOAIS ENTRE A EUROPOL E AS AUTORIDADES POLICIAIS BRASILEIRAS

 https://doi.org/10.36592/9786554600798-06

Lécio Silva Machado[1]

Jorge Alexandre Fagundes[2]

RESUMO

A pesquisa acadêmica desenvolvida tem como base o parecer emitido pela Autoridade Europeia para a Proteção de Dados (AEPD) a respeito da negociação de um acordo internacional entre a União Europeia (UE) e o Brasil. O acordo tem como objetivo viabilizar o intercâmbio de dados pessoais entre a Europol e as autoridades policiais brasileiras envolvidas na luta contra a criminalidade grave e o terrorismo. O estudo examinará as motivações subjacentes ao acordo, dadas as preocupações com a ameaça da criminalidade organizada na América Latina, ressaltando a relevância do Brasil no tráfico de drogas para a UE. A pesquisa adotará uma abordagem crítica e terá como base a revisão bibliográfica para explorar as diretrizes de negociação propostas pela Comissão, que buscam incorporar princípios cruciais de proteção de dados. A AEPD destaca a necessidade de preservar os direitos à privacidade e proteção de dados durante a troca de informações, sugerindo medidas como revisões periódicas da retenção de dados, garantias para o tratamento de dados sensíveis, supervisão humana em decisões automatizadas e transparência para os titulares dos dados. O objetivo principal do estudo é analisar o parecer da AEPD, enfocando a proteção de dados e privacidade no contexto do acordo entre a UE e o Brasil. A problemática central reside no equilíbrio entre a cooperação internacional contra o crime e a salvaguarda dos direitos fundamentais à privacidade e proteção de dados dos cidadãos afetados pelo compartilhamento de informações. A hipótese subjacente é que a implementação de salvaguardas apropriadas, em linha com as propostas da AEPD, pode possibilitar um acordo internacional eficaz entre a UE e o Brasil no intercâmbio de dados pessoais. O estudo explorará as diretrizes de negociação propostas, as recomendações da AEPD e a importância de equilibrar

[1] Doutorando em Ciências Jurídicas Criminais em Coimbra Portugal; Mestre em Direito pela UNIFLU, Especialista em Direito Penal Econômico e Europeu pelo IDPEE, Coimbra, Portugal; Professor universitário, Advogado especialista em Direito digital e criminal, parecerista, escritor do livro "Comentários à Lei Geral de Proteção de Dados", editora Lumen Juris; Escritor do E-book "Lei Geral de Proteção de Dados aplicada às Igrejas", DPO na OAB/ES, CRC/ES e no CRA/ES.

[2] Mestre em Negócios Internacionais pela Universidade de Ciência e Tecnologia de Miami - EUA, Advogado especialista em Direito Empresarial e digital, parecerista; Membro da ANADD - Associação Nacional dos Advogados de Direito Digital, Membro do Dtec – Estudos de Direito Digital e Proteção de Dados da Universidade Federal de Minas Gerais, UFMG; Coautor no livro Future Law, Vol. III, e Data protection Officer (DPO), certificado pelo instituto Holandês EXIN na LGPD, no GDPR e nas ISO 27001/27002. DPO na OAB/ES, CRC/ES e no CRA/ES.

segurança e privacidade em contextos de cooperação global. A pesquisa será embasada em fontes bibliográficas como o parecer da AEPD, as legislações de proteção e dados europeia (RGPD) e a brasileira (LGPD), as regulamentações pertinentes e análises acadêmicas abordando proteção de dados e cooperação policial internacional.
Palavras-chave: Europol, proteção de dados, cooperação internacional, criminalidade organizada, troca de informações.

1. INTRODUÇÃO

A busca por um acordo de cooperação internacional entre a Europol e as instituições policiais brasileiras tem suas motivações profundamente enraizadas na crescente preocupação com a criminalidade organizada na América Latina, com destaque para o papel do Brasil no combate ao tráfico de drogas em direção à União Europeia (EU). Este acordo é impulsionado pelo reconhecimento de que a cooperação internacional é essencial para combater eficazmente o crime transnacional, ao mesmo tempo em que é necessário garantir a proteção do direito à privacidade e à proteção de dados pessoais. As estatísticas alarmantes de crimes graves na América Latina, incluindo tráfico internacional de drogas, exploração de seres humanos, tráfico de pessoas, cibercriminalidade e terrorismo, representam sérias ameaças para os cidadãos da UE.

A Europol desempenha um papel crucial na avaliação e combate a essas ameaças, e a troca de informações com autoridades policiais brasileiras tornou-se essencial. No entanto, essa cooperação deve ser cuidadosamente equilibrada para respeitar os direitos individuais à privacidade e à proteção de dados pessoais. A Lei Geral de Proteção de Dados (LGPD) do Brasil e o Regulamento Geral de Proteção de Dados (RGPD) da UE estabelecem princípios fundamentais para a proteção de dados, e ambos os lados reconhecem a importância de autoridades independentes na supervisão das transferências de dados pessoais.

A Autoridade Europeia de Proteção de Dados (AEPD) desempenha um papel crítico na definição de diretrizes para garantir a integridade das informações e os direitos dos titulares de dados nesse acordo. A cooperação entre a AEPD e a Autoridade Nacional de Proteção de Dados (ANPD) do Brasil é fundamental para garantir a conformidade com as regulamentações de proteção de dados. Além disso,

a necessidade de estabelecer uma lista definida de crimes graves que permitiriam a troca de informações, bem como a revisão periódica da conservação de dados pessoais, destaca a importância de garantir o equilíbrio entre a aplicação da lei e a proteção da privacidade.

Por fim, é crucial assegurar que nenhuma decisão automatizada seja tomada com base nos dados recebidos no âmbito deste acordo sem a possibilidade de intervenção humana eficaz. Isso se baseia nos princípios de transparência, justiça e equidade, tanto na LGPD quanto no RGPD. A harmonização desses princípios e a supervisão por autoridades independentes são fundamentais para proteger os direitos das pessoas singulares aos dados pessoais e à privacidade em acordos internacionais. Essas medidas refletem um compromisso global com a proteção de dados pessoais, independentemente da localização geográfica, promovendo a segurança e a privacidade em um mundo cada vez mais conectado.

2. MOTIVAÇÕES PARA O ACORDO INTERNACIONAL

Explorar as motivações subjacentes à busca por um acordo internacional entre a UE e o Brasil é o foco deste capítulo. As preocupações com a criminalidade organizada na América Latina, com ênfase no papel do Brasil no combate ao tráfico de drogas para a EU talvez seja um dos maiores motivadores do presente acordo. Apontar de modo claro a importância da cooperação internacional na luta contra o crime transnacional e as expectativas das partes envolvidas nesse acordo é extremamente importante para entender como pode subsistir uma cooperação internacional que tem ao mesmo tempo que garantir a segurança entre várias nações, se preocupar com a proteção do direito à privacidade e à proteção dos dados pessoais.

A preocupação se fundamenta nos números alarmantes de ações de criminalidade organizada da América Latina em direção ao continente Europeu. Os chamados crimes graves, tráfico internacional de drogas, a exploração de seres humanos, o tráfico de pessoas, o contrabando de migrantes, atividades fraudulentas online e offline, assim como a criminalidade contra a propriedade, além do terrorismo

são os mais preocupantes e representam sérias ameaças aos habitantes da União Europeia.

Em 2021 a Europol publicou a Avaliação da Ameaça da Criminalidade Grave e Organizada (SOCTA) 3 , atualiza a comunidade europeia sobre a evolução da criminalidade grave e organizada e as ameaças que esta representa para a UE. A SOCTA é o resultado de uma colaboração sólida entre a Europol, as instituições de aplicação da lei dos países membros da União Europeia e outras partes interessadas, incluindo agências da UE, organizações internacionais e nações que não pertencem à UE, mas que têm acordos de cooperação com a Europol.

Entre os dados trazidos do SOCTA os mais alarmantes que podem ser citados é que perto de 40% das redes criminosas ativas na UE estão envolvidas no comércio de drogas ilegais e em sua maioria com drogas produzidas ou exportadas de países da América Latina.

Segundo o SOCTA,

> "quantidades sem precedentes de cocaína estão sendo contrabandeadas da América Latina para a União Europeia, resultando em lucros que chegam a bilhões de euros para os diversos criminosos envolvidos no comércio de cocaína em ambas as regiões, ou seja, na Europa e na América do Sul. O comércio de cocaína impulsiona organizações criminosas que, devido aos seus recursos substanciais, conseguem infiltrar e enfraquecer a economia, as instituições públicas e a sociedade da União Europeia."[4]

De fato, a cooperação no âmbito da segurança entre Brasil e a União Europeia é também ponto fundamental para a garantia da paz e da democracia. A instabilidade socioeconômica e democrática na América Latina e Caribe é vista também como ameaça à segurança da UE. A cooperação internacional na área de segurança tem ganhado importância desde a adoção da Estratégia da UE para a Segurança Cidadã na América Central e no Caribe em 2014.

---

[3] SOCTA *in* <https://www.europol.europa.eu/publications-events/main-reports/socta-report>.
[4] SOCTA, p.11.

No lado de cá do oceano Atlântico a situação é notória. O Brasil se destaca como a principal rota do tráfico de drogas produzidas na Bolívia, Peru, Equador e Venezuela para a União Europeia. AS apreensões de drogas são cada vez maiores, batendo recordes a cada nova operação da Polícia Federal.

Também há preocupação com as frequentes denúncias de tráfico de pessoas, tanto para a questão dos crimes sexuais como para a exploração do trabalho imigrante direcionados à Europa.

Os portos brasileiros são a porta escancarada de saída da criminalidade organizada para a União Europeia. A organizações criminosas criaram uma estrutura logística complexa para realizar o tráfico internacional de drogas. Essa estrutura envolve a produção da droga no exterior, o transporte para o território nacional, a distribuição interna e o envio de grandes quantidades de cocaína para o exterior, principalmente por meio do transporte marítimo. Os grupos atuam através da maioria dos portos marítimos do Brasil para enviar a droga para os portos da Europa. Ao todo, foram identificadas 21 apreensões no Brasil e no exterior, totalizando cerca de 17 toneladas de cocaína, todas vinculadas à atuação de uma só organização criminosa que atuava no porto de Santos.

A crescente ameaça da criminalidade organizada na América Latina, com ênfase no papel do Brasil no tráfico de drogas para a UE, surge como um dos principais impulsionadores desse acordo.

É evidente que a cooperação internacional desempenha um papel crucial na luta contra o crime transnacional, ao mesmo tempo em que visa proteger o direito à privacidade e à proteção dos dados pessoais. Portanto, a busca por soluções conjuntas para combater o tráfico de drogas e outras formas de criminalidade grave é crucial para ambas as regiões.

3. PROTEÇÃO DE DADOS E PRIVACIDADE NO ACORDO UE-BRASIL

Este capítulo analisa as implicações do acordo para a proteção de dados pessoais e a privacidade. Buscando entender as diretrizes de negociação propostas pela Comissão Europeia, que buscam incorporar princípios cruciais de proteção de dados. Identificando as recomendações da AEPD, que enfatizam a necessidade de

salvaguardas para garantir a integridade das informações e os direitos dos titulares dos dados.

Na Europa a Autoridade Europeia de Proteção de Dados, também conhecida como EDPS (European Data Protection Supervisor), é uma autoridade independente encarregada de supervisionar a proteção de dados pessoais dentro das instituições e órgãos da UE. Ela desempenha um papel importante na garantia de que as instituições da UE respeitem as regulamentações de proteção de dados, como o Regulamento Geral de Proteção de Dados.

A AEPD monitora e aconselha as instituições da UE em questões relacionadas à privacidade e proteção de dados, garantindo que o processamento de dados pessoais seja feito de acordo com os princípios estabelecidos no RGPD, como transparência, finalidade limitada, e consentimento informado dos titulares de dados. Além disso, a AEPD também desempenha um papel na emissão de diretrizes e pareceres sobre questões relacionadas à proteção de dados na UE.

A Autoridade Europeia emitiu cinco parecerem antes de 2022 sobre as sugestões da Comissão Europeia para iniciar discussões sobre tratados internacionais relacionados à transferência de informações pessoais entre a Europol, a agência da União Europeia responsável pela aplicação da lei, e as autoridades apropriadas de cinco nações latino-americanas: Equador, Brasil, Peru, Bolívia e México. O objetivo desses acordos é combater crimes graves e o terrorismo.

Os pareceres emitidos pela AEPD têm como finalidade oferecer orientação sobre como avançar com o estabelecimento de medidas de segurança para a proteção de dados em potenciais acordos internacionais, de forma a assegurar que as informações pessoais de indivíduos estejam resguardadas conforme os padrões estabelecidos pela União Europeia 5.

Em 22 de fevereiro de 2023, a Comissão Europeia 6 tomou uma decisão importante. Eles adotaram uma Recomendação de Decisão do Conselho que dá luz verde para iniciar negociações visando a celebração de um acordo entre a União Europeia e a República Federativa do Brasil sobre o compartilhamento de dados

[5] AEPD, 2023.
[6] A Comissão Europeia é uma das principais instituições da União Europeia (UE) e atua como o braço executivo da UE. Ela desempenha um papel crucial na formulação de políticas, na implementação de decisões e na gestão diária das atividades da UE.

pessoais de cidadãos das duas partes. Isso diz respeito à cooperação entre a Agência da União Europeia para a Cooperação Policial (Europol) e as autoridades brasileiras responsáveis pela luta contra crimes graves e terrorismo.

O propósito desta Recomendação é dar início às negociações com o Brasil para estabelecer um acordo internacional que permita a troca de dados pessoais entre a Europol e as autoridades policiais brasileiras que lidam com crimes graves e terrorismo. O documento anexo à Recomendação estabelece as orientações que o Conselho direciona à Comissão, delineando os objetivos que a Comissão deve perseguir em nome da União Europeia durante as negociações.

A AEPD já havia apresentado observações em 2018 e 2020 sobre a troca de dados pessoais entre a Europol e as autoridades policiais de países terceiros com base no Regulamento Europol.

Com base nesta Recomendação, em 03 de maio de 2023 a AEPD emitiu parecer 14/2023 favorável a negociação de um acordo internacional sobre intercâmbio de dados pessoais entre a Europol e as autoridades policiais brasileiras destacando a importância de garantir controles adequados em relação à proteção de dados pessoais no futuro acordo entre a UE e o Brasil. Suas recomendações visam esclarecer e, se necessário, desenvolver essas garantias e controles. Elas não impedem futuras recomendações com base em informações adicionais disponíveis e nas disposições do projeto de acordo durante as negociações.

A AEPD enfatiza que é de extrema importância para a futura troca de informações a supervisão por uma autoridade independente desempenhando um papel fundamental no que diz respeito ao direito à proteção de dados pessoais. Neste sentido, a entrada em vigor da Lei Geral de Proteção de Dados Pessoais[7] que estabeleceu a criação da Autoridade Nacional de Proteção de Dados[8] representou um passo positivo no sentido de fortalecer a proteção da privacidade e dos dados pessoais no país.

[7] Lei nº 13.709/2018.

[8] Entidade autônoma e independente do governo federal do Brasil, criada para supervisionar e regulamentar questões relacionadas à proteção de dados pessoais no país. A ANPD foi estabelecida pela Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que entrou em vigor em setembro de 2020, inspirada em regulamentações europeias, como o Regulamento Geral de Proteção de Dados (RGPD).

O próprio diretor da AEPD Wojciech Wiewiórowski, escolhido para a gestão do órgão entre 2019 à 2024, destaca que

> "Congratulo-me com o facto de a Comissão ter estabelecido até agora – também com base em pareceres anteriores da AEPD – um conjunto bem estruturado de objetivos a alcançar aquando da negociação de acordos sobre o intercâmbio de dados pessoais entre a Europol e as autoridades responsáveis pela aplicação da lei de países terceiros. As circunstâncias particulares de cada jurisdição estrangeira, como a existência de uma autoridade independente de proteção de dados ou a adesão à Convenção n.º 108 do Conselho da Europa, devem ser sempre devidamente tidas em conta."9

A Europa é uma região com intensa transferência de dados pessoais para outros países. Empresas europeias frequentemente enviam dados para o Brasil e outras nações. A existência da ANPD e da LGPD significa que, ao transferir dados pessoais para o Brasil, as empresas europeias precisam considerar as regulamentações brasileiras, incluindo a proteção de dados, para garantir o cumprimento das leis locais. Isso ressalta a importância de uma legislação forte de proteção de dados em países fora da União Europeia.

Embora a ANPD seja uma autoridade brasileira, ela pode cooperar com outras autoridades de proteção de dados em todo o mundo, incluindo a AEPD. Isso é importante em casos de investigações transnacionais ou questões relacionadas à proteção de dados que envolvam jurisdições múltiplas. A cooperação internacional entre autoridades de proteção de dados ajuda a garantir a aplicação consistente das leis de privacidade e proteção de dados.

Vale destacar que o Regulamento Europol proíbe explicitamente o tratamento pela Europol de "qualquer informação que tenha sido claramente obtida em clara violação dos direitos humanos"10. Por conseguinte, a AEPD recomenda que o futuro Acordo exclua explicitamente as transferências de dados pessoais obtidos em violação manifesta dos direitos humano.

---

[9] AEPD (2023).

[10] Veja art.23.9 do Regulamento da Europol. DIsponível em: in < https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0794> Acessado em 28 ago 2023.

Tratando diretamente do parecer da AEPD sobre a troca de dados entre os órgãos de polícia da União Europeia e do Brasil, destaca-se entre os pontos mais importantes que determinaram a emissão do parecer o estabelecimento de uma lista das infrações penais que seriam passíveis de trocas de informações entre os órgãos de segurança pública. Tal medida visa garantir quer a violação do direito a privacidade e a proteção de dados não esteja sujeita a qualquer tipo de investigação criminal, mas sim a uma espécie de investigação de crimes graves e terrorismo. É extremamente importante que entre estes crimes estejam ao menos o Tráfico de drogas internacional, tráfico de pessoas, tráfico de armas, cibercriminalidade, terrorismo e investigação de organizações criminosas multinacionais que atuem na lavagem e dinheiro e corrupção conexas a aqueles crimes.

A determinação de uma lista definida de crimes que permitiriam a violação dos direitos à privacidade e a proteção de dados não impede que ocorra uma revisão constante da dos crimes que porventura possam fazer parte do rol dos crimes graves.

Outro ponto que cabe listar é a revisão periódica da necessidade de conservação dos dados pessoais transferidos em bancos de dados da Europol ou das autoridades policiais do Brasil, tendo em vista que o compartilhamento e arquivamento de dados está baseado na existência de uma finalidade legal, ou seja, havendo o fim de uma investigação que necessitou de compartilhamento de dados entre os órgãos de segurança, as informações trocadas devem ser excluídas, a fim de garantir novamente a privacidade e proteção dos dados pessoais, podendo em todos os casos estabelecer outras finalidades que justifiquem a manutenção dos dados utilizados. Certo é que a limitação da finalidade está entre os princípios fundamentais do quadro de proteção de dados da EU e do Brasil.

Baseado no art. 31º do Regulamento da Europol a organização policial europeia deve conduzir avaliações periódicas a cada 03 (três) anos para determinar a necessidade e a adequação do armazenamento de dados pessoais em seu poder. Qualquer decisão de manter os dados além dos primeiros três anos deve ser cuidadosamente justificada e devidamente registrada. Além disso, a Europol é obrigada a remover os dados assim que for informada de que esses foram excluídos dos sistemas do fornecedor de dados. Assim, esclarece a AEPD que regras como

essas façam parte dos futuros acordos celebrados no âmbito da cooperação internacional, garantindo assim a periódica análise quanto ao armazenamento, revisão, correção e eliminação de dados pessoais trocados. Este último ponto é muito preocupante no que tange ao Brasil, já que as organizações policiais brasileiras não têm legislações mínimas quanto ao tratamento de dados pessoais em caso de investigação criminal.

Uma das principais preocupações no contexto da investigação criminal e a proteção de dados no Brasil ainda é como as agências policiais coletam, armazenam e compartilham informações pessoais durante investigações criminais. É essencial que haja protocolos rigorosos para garantir que apenas informações relevantes sejam acessadas e utilizadas, respeitando os princípios de finalidade e consentimento informado dos titulares de dados. Além disso, é necessário que as agências policiais tenham medidas técnicas e organizacionais robustas para proteger esses dados contra vazamentos e violações.

Importante é equilibrar a necessidade de investigação e aplicação da lei com a proteção da privacidade e dos direitos dos cidadãos, principalmente no contexto de troca de dados pessoais com outros órgãos internacionais como a Europol. Isso exige um cuidadoso equilíbrio entre a obtenção de informações relevantes para investigações criminais e a garantia de que os direitos de privacidade dos indivíduos sejam preservados.

Na salvaguarda dos dados pessoais compartilhados entre Europol de as polícias do Brasil, deve ficar bem clara a obrigação de garantir a segurança dos dados pessoais através de medidas técnicas e organizativas adequadas, permitindo que apenas pessoas autorizadas tenham acesso aos dados pessoais, bem como a obrigação de notificação em caso ocorra uma violação de dados pessoais que afete os dados transferidos entre as instituições policiais.

Não se deve perder de vista a necessidade ainda de determinar como será garantido ao titular de dados o acesso a informação sobre seus dados pessoais tratados após a troca de informações. É importante determinar um canal de fácil comunicação aos cidadãos do Brasil e da Europa ao exercício de seus direitos de titular para ter acesso, retificação e apagamento, incluindo os fundamentos

específicos que poderá permitir quaisquer restrições necessárias e proporcionais, sem ferir a privacidade e a proteção de dados pessoais.

Neste contexto, a Autoridade Europeia de Proteção de Dados sugeriu ainda em seu parecer que as partes envolvidas devem realizar trocas regulares de informações sobre o exercício dos direitos pelos titulares de dados. Isso inclui o compartilhamento de estatísticas que abrangem o número de solicitações feitas e seus resultados, especificamente quantos casos envolveram restrições desses direitos. Além disso, as partes podem concordar em compartilhar informações relevantes relacionadas à utilização dos mecanismos de supervisão e recursos associados à implementação do Acordo.

Por fim, deve ser assegurado no caso de troca de dados pessoais pelos órgãos policiais que nenhuma decisão automatizada seja tomada com base nos dados recebidos ao abrigo de um futuro acordo entre a Europol e a Polícia brasileira sem a possibilidade de intervenção humana eficaz, isto com fundamento em princípios cruciais de proteção de dados. Um dos princípios mais importantes é o da transparência, que exige que os processos de tomada de decisão automatizada sejam claros e compreensíveis para os titulares de dados. Isso inclui a compreensão de como e por que uma decisão foi tomada. Além disso, o princípio da justiça e equidade implica que os indivíduos tenham a oportunidade de contestar ou contestar as decisões automatizadas que os afetem.

Tanto a LGPD quanto o RGPD compartilham o compromisso com os direitos dos titulares de dados e a necessidade de garantir a justiça nas decisões automatizadas. A LGPD do Brasil, em seu Artigo 20, confere aos titulares de dados o direito de revisar decisões automatizadas e exige a explicação da lógica utilizada nesses processos, sendo que da mesma forma, o RGPD europeu, em seu Artigo 22, estabelece que os indivíduos têm o direito de não serem submetidos a decisões automatizadas exclusivamente com base no tratamento automatizado, a menos que haja exceções específicas ou o consentimento dos titulares de dados.

Portanto, ambas as legislações se alinham na importância de garantir que as decisões automatizadas respeitem os direitos dos titulares de dados e que haja um mecanismo eficaz para intervenção humana, quando necessário, para garantir justiça e equidade nas decisões que afetam os indivíduos. Esses princípios são

fundamentais para proteger a privacidade e os direitos dos cidadãos, independentemente de onde estejam localizados, promovendo uma abordagem global para a proteção de dados pessoais.

A supervisão das transferências de dados pessoais no contexto de acordos internacionais é uma questão crítica para a proteção dos direitos das pessoas singulares aos dados pessoais e à privacidade. Tanto a LGPD quanto o RGPD destacam a importância do controle por autoridades independentes nesse processo. No RGPD, o Artigo 46 estabelece a necessidade de garantir a proteção adequada dos dados pessoais em transferências para países fora da União Europeia, e isso envolve a atuação de autoridades de supervisão.

A AEPD enfatiza a troca regular de informações entre as partes envolvidas nos acordos internacionais como uma medida crucial para facilitar a aplicação de medidas adequadas de proteção de dados. Isso está em linha com os princípios de transparência e cooperação entre as autoridades de proteção de dados, conforme estabelecido no RGPD. Além disso, a LGPD no Brasil estabelece a importância da supervisão por autoridades independentes, como ANPD, para garantir o cumprimento das regulamentações de proteção de dados em acordos internacionais e a proteção dos direitos dos titulares de dados.

Portanto, a harmonização entre a LGPD e o RGPD na necessidade de autoridades independentes eficazes e na troca de informações periódicas para supervisionar as transferências de dados pessoais em acordos internacionais, principalmente naqueles ligados à investigação criminal, é fundamental para garantir a proteção dos direitos individuais à privacidade e à proteção de dados em contextos globais. Essas medidas contribuem para a construção de um ambiente onde os direitos dos titulares de dados são respeitados independentemente de onde esses dados sejam transferidos.

CONCLUSÃO

Em conclusão, a análise do acordo entre a União Europeia (UE) e o Brasil em relação à proteção de dados pessoais e privacidade revela uma série de pontos críticos a serem considerados. A AEPD desempenha um papel fundamental na

supervisão e aconselhamento em questões de privacidade e proteção de dados na UE, garantindo que os princípios estabelecidos no Regulamento Geral de Proteção de Dados (RGPD) sejam respeitados.

A decisão de iniciar negociações para compartilhamento de dados pessoais entre a Europol e as autoridades brasileiras é uma etapa importante, com a AEPD emitindo um parecer favorável, destacando a necessidade de garantir controles adequados para a proteção de dados no acordo. A existência LGPD e da ANPD no Brasil fortalece a proteção da privacidade e dos dados pessoais no país.

É crucial definir uma lista de infrações penais que justifiquem a troca de informações entre os órgãos de segurança, visando equilibrar a proteção da privacidade com a investigação de crimes graves e terrorismo. Além disso, a revisão periódica da necessidade de conservação de dados pessoais compartilhados é essencial para garantir o cumprimento dos princípios de finalidade limitada.

Medidas técnicas e organizativas adequadas são necessárias para garantir a segurança dos dados pessoais, juntamente com um canal de comunicação claro para que os titulares de dados possam exercer seus direitos de acesso, retificação e apagamento. A transparência na troca de informações sobre o exercício dos direitos dos titulares de dados é fundamental para manter a privacidade e a proteção de dados pessoais.

Em resumo, a cooperação internacional em relação à proteção de dados pessoais envolve a consideração cuidadosa de vários aspectos, incluindo a salvaguarda dos direitos dos indivíduos, a segurança dos dados e a revisão constante das práticas de compartilhamento. Esses são passos cruciais para garantir que a troca de informações entre a UE e o Brasil seja feita de maneira justa e respeitosa da privacidade.

REFERÊNCIAS

AEPD (2023). **Os acordos internacionais para combater o crime exigem fortes salvaguardas de proteção de dados.** in <https://edps.europa.eu/press-publications/press-news/press-releases/2023/international-agreements-fight-crime-require-strong-data-protection-safeguards_en> Acessado em 29 ago 2023.

AEPD (2023). **Parecer 14/2023 da AEPD sobre o mandato de negociação para a celebração de um acordo internacional sobre o intercâmbio de dados pessoais entre a Europol e as autoridades brasileiras responsáveis pela aplicação da lei**. *in* <https://edps.europa.eu/data-protection/our-work/publications/opinions/2023-05-03-edps-opinion-142023-negotiating-mandate-conclude-international-agreement-exchange-personal-data-between-europol-and-brazilian-law-enforcement_en> Acessado em 28 ago 2023.

AEPD (2023). **Resumo do parecer da Autoridade Europeia para a Proteção de Dados sobre o mandato de negociação para celebrar um acordo internacional sobre o intercâmbio de dados pessoais entre a Europol e as autoridades policiais brasileiras. 2023/C 199/06**. Bruxelas. 03 mai 2023. in <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=uriserv%3AOJ.C_.2023.199.01.0010.01.POR&toc=OJ%3AC%3A2023%3A199%3AFULL> Acessado em 01 set 2023.

BRASIL (2017). **Acordo de Cooperação Estratégica entre a República Federativa do Brasil e a Europol**. Assinado em 11 abr 2017. in <https://www.europol.europa.eu/partners-collaboration/agreements/brazil>. Acessado em 18 set 2023.

BRASIL (2018). Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Lei do Marco Civil da Internet). Diário Oficial da União. <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm> Acessado em 28 ago 2023.

EUROPOL (2021), **Avaliação da ameaça da criminalidade grave e organizada da União Europeia, Uma influência corruptora: a infiltração e o enfraquecimento da economia e da sociedade da Europa pelo crime organizado, Serviço de Publicações da União Europeia, Luxemburgo.** *in* https://www.europol.europa.eu/publications-events/main-reports/socta-report Acessado em 01 set 2023.

FRAZÃO, Ana. TEPEDINO, Gustavo. OLIVA, Milena Donato. (Orgs). **Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro.** 1. Ed. São Paulo: Revista dos Tribunais, 2019.

GONÇALVES, Tânia Carolina Nunes Machado. **Gestão de Dados Pessoais e Sensíveis pela Administração Pública Federal: desafios, modelos e principais impactos com a nova Lei.** Orientador Prof. Dr. Marcelo Dias Varella. – Brasília, 2019. in <https://www.uniceub.br/arquivo/144ng_20190730051313*pdf?AID=3007> Acesso 12 jan. 2020.

GUIMARÃES, João Alexandre Silva Alves. MACHADO. Lécio Silva. **Comentários a lei geral de proteção de dados.** 1 Ed. Rio de Janeiro : Lumen Juris, 2020.

OBSERVATÓRIO EUROPEU DA DROGA E DA TOXICODEPENDÊNCIA (2023), **Relatório Europeu sobre Drogas 2023: Tendências e Desenvolvimentos , <https://www.emcdda.europa.eu/publications/european-drug-report/2023_en> Acessado em 01 set 2023.**

POLICIA FEDERAL (2023). **PF desarticula organização investigada pelo envio de 17 toneladas de cocaína para a Europa.** in <https://www.gov.br/pf/pt-br/assuntos/noticias/2023/08/pf-desarticula-organizacao-investigada-pelo-envio-de-17-toneladas-de-cocaina-para-a-europa> Acessado em 02 set 2023.

UNIÃO EUROPEIA. (2018). **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral de Proteção de Dados).** *in* <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679> Acessado em 28 de ago 2023.

7. REPERCUSSÕES DO JULGAMENTO DA ADI Nº 6.649 E DA ADPF Nº 695: SEPARAÇÃO INFORMACIONAL DE PODERES E LIMITES DO COMPARTILHAMENTO DE DADOS PESSOAIS

https://doi.org/10.36592/9786554600798-07

Lucia Maria Teixeira Ferreira[1]

RESUMO

À luz da decisão proferida pelo Supremo Tribunal Federal no julgamento conjunto da Ação Direta de Inconstitucionalidade nº 6.649/DF e da Ação de Descumprimento de Preceito Fundamental n.º 695/DF, este artigo estuda a importância do princípio da separação informacional de poderes como uma atualização do princípio da separação de poderes na era informacional e como uma exigência do Estado Democrático de Direito. Em face da normativa constitucional e da Lei Geral de Proteção de Dados Pessoais (LGPD), o compartilhamento de dados pessoais em poder do Estado não pode ser feito indiscriminadamente em nome da "eficiência" para políticas públicas que não foram previamente esclarecidas. Todo compartilhamento deve seguir parâmetros de adequação, proporcionalidade e necessidade, com bases legais e finalidades apropriadas, bem como medidas de segurança e transparência que garantam a proteção dos direitos dos cidadãos.
Palavras-chave: Proteção de dados pessoais. Separação Informacional de Poderes.

Introdução

Pretende-se discutir o alcance e a extensão da decisão do Supremo Tribunal Federal na Ação Direta de Inconstitucionalidade n.º 6.649/DF, julgada conjuntamente com a Ação de Descumprimento de Preceito Fundamental n.º 695/DF, no tocante ao compartilhamento de dados pessoais pelos órgãos estatais e aos eventuais riscos que a utilização de tecnologias da informação pelo Estado (e em parcerias e

---

[1] Membra da Comissão Especial de Proteção de Dados do CFOAB. Coordenadora de Estudos e Pareceres da Comissão de Proteção de Dados e Privacidade da OAB/RJ. Doutoranda em Direito Constitucional no Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP). Mestre em Direito Civil pela Universidade do Estado do Rio de Janeiro (UERJ). Pós-Graduada em Sociologia Urbana pelo Departamento de Ciências Sociais da UERJ. Professora e Membra da ABRADEP. Procuradora de Justiça aposentada do Ministério Público do Rio de Janeiro (MPRJ). Advogada. E-mail: luciaferreira@infolink.com.br. Currículo Lattes: http://lattes.cnpq.br/885 9827696202938.

convênios do Estado com empresas privadas) pode acarretar para os direitos fundamentais, notadamente à privacidade, à proteção de dados pessoais e à autodeterminação informativa. Serão analisados os fatos e fundamentos que embasaram os pedidos nessas ações de controle concentrado de constitucionalidade, bem como o resultado do julgamento, com a síntese dos fundamentos da decisão.

Como destaca Laura Schertel Mendes, é decisivo para a concepção da proteção de dados e do direito à autodeterminação informativa "o princípio segundo o qual não mais existiriam dados insignificantes nas circunstâncias modernas do processamento automatizado de dados", de modo que "o risco do processamento de dados residiria mais na finalidade do processamento e nas possibilidades de processamento do que no tipo dos dados tratados"[2] (ou no fato de quão sensíveis ou íntimos eles são).

Ingo Sarlet e Gabrielle Sales Sarlet defendem que a separação informacional de poderes é um princípio fundamental estruturante implicitamente positivado pela Constituição Federal, que vincula toda a atuação do Estado brasileiro, como norma de eficácia direta, devendo ser concretizado pelo legislador, exigindo-se a motivação das decisões relativas a tratamento de dados. Além disso, afirmam que a separação informacional de poderes consiste em uma ressignificação da semântica do princípio da divisão de poderes à luz do constitucionalismo digital, o que implica em uma separação nítida entre as diversas áreas de atuação estatal sob pena de descumprimento de um preceito fundamental e de violação das exigências do Estado Democrático de Direito.[3]

> *É nesse contexto que se pode e deve extrair, em especial do artigo 1º, caput (Estado Democrático de Direito), artigo 1º, III (dignidade da pessoa humana), artigo 1º, § único (soberania popular), bem como do artigo 2º (separação de poderes), da CF, dois princípios implícitos, nucleares e estruturantes para a*

---

[2] MENDES, Laura Schertel. Autodeterminação informativa: a história de um conceito. **Pensar**, Fortaleza, v. 25, n. 4, p. 1-18, out./dez. 2020, p. 11.

[3] SARLET, Ingo Wolfgang; SALES SARLET, Gabrielle. **Separação informacional de poderes no direito constitucional brasileiro**. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2022, p. 28. Disponível em: file:///C:/Users/msgar/Downloads/DataPrivacy.-Separacao-Informacional-de-Poderes.-2022.pdf. Acesso em: 3 out. 2023.

> *atuação estatal, designadamente, o princípio (e direito fundamental) do devido processo informacional e o princípio da separação informacional de poderes*. Ambos, por sua vez, devem ser concretizados pelos atores estatais, ademais de serem interpretados e aplicados em conjugação com outros diplomas legais já em vigor, como é o caso da LAI (Lei de Acesso à Informação) e da LGPD, que, na dicção do artigo 23, prescreve que o tratamento de dados pessoais pelas pessoas jurídicas de direito público deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.[4]

A decisão proferida pelo STF na ADI n.º 6.649 e na ADPF n.º 695 representa um marco importante para a afirmação do princípio da separação informacional de poderes, visto que seus fundamentos atualizam o princípio da separação de poderes na era informacional como uma exigência do Estado Democrático de Direito. Em face da normativa constitucional e da Lei Geral de Proteção de Dados Pessoais (LGPD),[5] o compartilhamento de dados pessoais em poder do Estado não pode ser feito indiscriminadamente em nome da "eficiência" para políticas públicas que não foram previamente esclarecidas. Todo compartilhamento deve seguir parâmetros de adequação, proporcionalidade e necessidade, com bases legais e finalidades apropriadas, bem como medidas de segurança e transparência que garantam a proteção dos direitos dos cidadãos.

---

[4] SARLET, Ingo Wolfgang; SALES SARLET, Gabrielle. **Separação informacional de poderes no direito constitucional brasileiro**. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2022, p. 39. Disponível em: file:///C:/Users/msgar/Downloads/DataPrivacy.-Separacao-Informacional-de-Poderes.-2022.pdf. Acesso em: 3 out. 2023.

[5] BRASIL, **Lei n.º 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Presidência da República, Brasília, DF. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 4 out. 2023

1. Apresentação Dos Casos

1.1 *A ADI nº 6.649/DF (o caso do Cadastro Base do Cidadão)*

Em 10 de outubro de 2019, foi publicado no Diário Oficial da União o Decreto n.º 10.046/2019, que "dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados".[6] Até a edição do referido decreto, o modelo de compartilhamento de dados na administração federal era aquele definido pelo Decreto n.º 8.789/2016,[7] regulamentado pela Portaria nº 58/2016,[8] da Secretaria de Tecnologia da Informação.

O Decreto n.º 8.789/2016 foi revogado pelo Decreto n.º 10.046/2019, o qual, em conjunto com outra deliberação do Chefe do Poder Executivo Federal (Decreto n.º 10.047/2019[9]), criou uma gigantesca e unificada base de dados dos cidadãos. No Decreto n.º 10.046/2019, não ficaram claras as finalidade do compartilhamento tampouco o modo como os dados pessoais seriam compartilhados pelos órgãos e entidades do governo federal, bem como pelos demais Poderes da República.

Autoridades governamentais afirmaram que as medidas previstas no Decreto n.º 10.046/2019, especialmente o Cadastro Base do Cidadão, facilitariam o acesso

---

[6] BRASIL. **Decreto n. 10.046, de 9 outubro 2019**. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Presidência da República, Brasília, DF. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 4 out. 2023.

[7] BRASIL. **Decreto n.º 8.789, de 29 de junho de 2016**. Dispõe sobre o compartilhamento de bases de dados na administração pública federal. Presidência. Presidência da República, Brasília, DF. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8789.htm. Acesso em: 4 out. 2023.

[8] BRASIL. Ministério do Planejamento, Desenvolvimento e Gestão. Secretaria de Tecnologia da Informação. **Portaria n.º 58, de 23 de dezembro de 2016**. Dispõe sobre procedimentos complementares para o compartilhamento de bases de dados oficiais entre órgãos e entidades da administração pública federal direta e indireta e as demais entidades controladas direta ou indiretamente pela União. Brasília, DF. Disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/portarias-federais/portaria-no-58-de-23-de-dezembro-de-2016. Acesso em: 4 out. 2023.

[9] BRASIL. **Decreto n. 10.047, de 9 outubro 2019**. Dispõe sobre a governança do Cadastro Nacional de Informações Sociais e institui o programa Observatório de Previdência e Informações, no âmbito do Cadastro Nacional de Informações Sociais. Presidência da República, Brasília, DF. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d10047.htm. Acesso em 4 out. 2023.

dos brasileiros a serviços governamentais no formato digital. Certamente, a digitalização e a desburocratização dos serviços públicos são necessárias e tais medidas são uma antiga reivindicação da população brasileira. Contudo, as regras previstas no decreto encontravam-se em descompasso com os pilares e paradigmas normativos da legislação federal pertinente e com as normas constitucionais atinentes à matéria.

Com base no entendimento de que o ato normativo do Poder Executivo extrapolou o seu poder regulamentar, foram apresentados, no Congresso Nacional, cinco Projetos de Decreto Legislativo com o objetivo de sustar o Decreto n.º 10.046/2019. Com fundamento no art. 49 da Constituição Federal, o Congresso Nacional pode "sustar atos do Poder Executivo que exorbitem o poder regulamentar ou os limites da delegação legislativa". Evidentemente, a criação da megabase de dados, da forma como foi disciplinada pelo decreto do Presidente da República, exigia que o Parlamento discutisse urgentemente esse tema e as consequências de tal norma infralegal, mas os Projetos de Decreto Legislativo não prosperaram e a questão acabou sendo levada ao Supremo Tribunal Federal em sede de ações de controle concentrado de inconstitucionalidade.

O Conselho Federal da OAB (CFOAB) promoveu intensas discussões sobre o tema, iniciados na Comissão de Proteção de Dados e Privacidade do Rio de Janeiro sob a presidência da Dra. Estela Aranha, com a formulação de um parecer sobre a inconstitucionalidade do Decreto nº 10.046/2019[10] e a elaboração de outro parecer por parte da Comissão de Estudos Constitucionais do CFOAB, da lavra do Dr. Ilton Noberto Robl Filho, que também sustentou a inconstitucionalidade do aludido decreto. Após meses de estudos e debates, o CFOAB propôs a ADI nº 6.649/DF, no dia 21 de dezembro de 2020.

Na ADI n.º 6.649, o CFOAB sustentou que o ato normativo impugnado padece de "a) inconstitucionalidade formal, por afronta ao artigo 84, incisos IV e VI, 'a', da Constituição Federal, visto que este decreto inova no ordenamento jurídico, tendo o Presidente da República extrapolado a sua competência constitucional regulamentar

[10] FERREIRA, Lucia Maria Teixeira. Parecer sobre a legalidade dos Decretos 10.046/2019 e 10.047/2019 em face das normas que disciplinam os direitos fundamentais à proteção de dados e à privacidade no ordenamento jurídico brasileiro. **Revista do Ministério Público do Estado do Rio de Janeiro**. n. 75, p. 258-259, jan./mar 2020.

ao editar este ato infralegal; b) inconstitucionalidade material, por violação direta aos artigos 1º, inciso III, e 5º, caput, incisos X e XII e LXXII da Constituição Federal, os quais asseguram, respectivamente, a dignidade da pessoa humana; a inviolabilidade da intimidade, da privacidade e da vida privada, da honra e da imagem das pessoas; o sigilo dos dados; a garantia do habeas data enquanto instrumento de tutela material do direito à autodeterminação informativa; e por ferimento aos direitos fundamentais à proteção de dados pessoais e à autodeterminação informativa, reconhecidos como direitos fundamentais autônomos, com fulcro nos arts. 1º, inciso III, e 5º, caput, e incisos X, XII e LXXII da Constituição Federal, através da decisão proferida pelo Plenário dessa Egrégia Corte nos autos da Ação Direta de Inconstitucionalidade 6.387".

Os principais fundamentos fáticos e jurídicos do CFOAB na petição inicial da ADI 6.649 foram os seguintes:

> a) As regras adotadas para o compartilhamento de dados pelos órgãos governamentais permitem interligar bases e cruzar dados pessoais *sem critérios que sejam conhecidos dos cidadãos*: sem informações claras, adequadas e transparentes sobre a realização da coleta e do tratamento, bem como, sobre quem são e como agem os agentes do tratamento. Ademais, não existem considerações sobre ponto essencial do regime de proteção de dados pessoais instituído pelo respectivo direito fundamental e consolidado em legislação, que é a verificação se o compartilhamento de dados entre órgãos públicos estaria em consonância com a finalidade para a qual a informação pessoal foi originariamente coletada.
> b) O sistema de controle dos agentes de tratamento é totalmente falho, de forma a fragilizar os direitos fundamentais. O referido Decreto é silente quanto à elaboração de relatórios de impacto de proteção de dados e sequer evidencia os mecanismos adequados de segurança da informação. E o "gestor de dados" também não se compatibiliza com a figura do encarregado de tratamento de dados pessoais, conforme o disposto no art. 23, inciso III, da LGPD.
> c) O direito à autodeterminação informativa será enfraquecido pela interligação de bases de dados e a permissão do seu cruzamento sem critérios prévia e devidamente esclarecidos. Os titulares dos dados serão privados de informações

claras, adequadas e facilmente acessíveis sobre a coleta e a realização do tratamento dos dados. E ainda causa maior temor a eventual implementação de programas futuros de compartilhamento através de convênios de acesso com empresas privadas – que se conectariam a esses dados pessoais através do cadastro centralizado, como um gigantesco *data lake*.

d) O cidadão estaria obrigado a aceitar a coleta estatal de um dado pessoal para uma estipulada finalidade (como a execução de uma determinada política pública), com base no art. 7º, inciso III, da LGPD. Contudo, viveria em um regime de permanente insegurança, posto que o dado coletado mediante aquela finalidade poderia ser utilizado seguidamente para uma outra finalidade e assim sucessivamente, sem o seu conhecimento, representando uma situação de risco para os titulares. Isto viola a Constituição Federal e a LGPD, bem como está em total desconformidade com as regras e os padrões internacionais de proteção de dados.

e) A LGPD prevê que o tratamento e compartilhamento de dados pela administração pública, dentre as hipóteses elencadas nas bases legais do art. 7º, restringe-se aos dados necessários para a execução daquela determinada política pública, e não para uma cadeia indefinida e indeterminada de finalidades inadequadas e/ou obscuras. A impossibilidade de se verificar a real finalidade do compartilhamento de dados é um aspecto que vulnera ainda mais o titular de dados pessoais. Nesse sentido, a própria amplitude dos órgãos envolvidos e sua heterogeneidade – conforme o art. 1º do Decreto, "entidades da administração pública federal direta, autárquica e fundacional e os demais Poderes da União" – representa uma situação de intenso risco para os titulares dos dados.

f) O Decreto 10.046/2019 cria novos conceitos de dados pessoais alheios à LGPD e amplia a coleta de dados pessoais sensíveis sem as devidas salvaguardas, uma vez que as chamadas base integradora e base temática (art. 2º, incisos VI e VII) – *bases que integrarão os atributos biográficos previstos no art. 2º, I, e os atributos biométricos previstos no art. 2º, II* – provocam indagações sobre o contexto em que ocorrerão o tratamento e a utilização dessas novas bases e o cruzamento desses dados. Tais informações podem ser utilizadas para a criação de um sistema de vigilância massivo e para o controle político intenso dos cidadãos, típico de regimes totalitários.

> g) O Decreto apresenta sérios problemas de governança, posto que o Comitê Central de Governança seria composto apenas por órgãos do governo federal, sem qualquer participação de entidades da sociedade civil. Além disso, a ausência da Autoridade Nacional de Proteção de Dados nas decisões e na supervisão do Comitê Central de Governança estaria em descompasso com a LGPD, criando a possibilidade de decisões contraditórias de órgãos governamentais superpostos, decisões estas que poderão ser extremamente prejudiciais para os titulares de dados pessoais.

Na petição exordial da ADI n.º 6.649, o CFOAB suscitou a preliminar de prevenção para distribuição por dependência daquela ação direta de inconstitucionalidade à ADPF n.º 695/DF (conhecida como Caso ABIN-Denatran), em face da prevenção:

> Preliminarmente, o autor requer a distribuição por dependência desta petição inicial à Ação de Descumprimento de Preceito Fundamental nº 695/DF, ajuizada pelo Partido Socialista Brasileiro (PSB) em junho de 2020, cujo relator é o Eminente Ministro Gilmar Mendes, o qual se tornará prevento para o julgamento de ambos os processos, nos termos do que dispõe o art. 69 do RISTF: "A distribuição da ação ou do recurso gera prevenção para todos os processos a ele vinculados por conexão ou continência". A causa de pedir desta ação direta de inconstitucionalidade possui conexão com a causa de pedir da supracitada ADPF, haja vista que ambas discutem questões relativas à privacidade, à proteção de dados pessoais, ao compartilhamento de dados pelo Poder Público e à constitucionalidade do Decreto nº 10.046/2019, devendo os feitos ser reunidos para julgamento conjunto a fim de que não sejam proferidas decisões conflitantes ou contraditórias.

A preliminar de prevenção foi aceita e o Relator, Ministro Gilmar Mendes, adotou para ambos os feitos o rito do art. 12 da Lei n.º 9.868/1999.[11] O Presidente

---

[11] Lei n.º 9.868/1999, art. 12: "Havendo pedido de medida cautelar, o relator, em face da relevância da matéria e de seu especial significado para a ordem social e a segurança jurídica, poderá, após a prestação das informações, no prazo de dez dias, e a manifestação do Advogado-Geral da União e do

da República prestou informações defendendo o "não conhecimento da presente ação direta de inconstitucionalidade, ante a inadequação da via eleita" e o "reconhecimento da ausência de inconstitucionalidade formal ou material, bem como da licitude do compartilhamento de dados, nos moldes como previsto no Decreto nº 10.046/2019".

Foram admitidos, na condição de *amicus curiae*, a Associação Data Privacy Brasil de Pesquisa, o Laboratório de Políticas Públicas e Internet LAPIN e o Instituto Mais Cidadania.

Danilo Doneda foi um dos signatários da petição inicial do CFOAB e fez a sustentação oral em nome da parte autora, no Plenário do STF, no dia 31 de agosto de 2022. Referindo-se à decisão histórica na ADI 6.387/DF, na qual também fora um dos signatários de uma das ações propostas pelos partidos políticos, Doneda destacou que

> O Decreto, no entanto, como se a modernidade lhe fosse estranha ou inconveniente, parece ignorar este novo paradigma ao considerar a informação pessoal sob prisma meramente utilitarista e tecnocrático, em frontal desacordo com o que afirmou esta Excelsa Corte em julgamento paradigmático de 2020 quando da propositura por este CF-OAB e por uma série de partidos políticos de ADIs em face da MP954, que pretendia justamente o compartilhamento de dados pessoais entre dois entes públicos sem maiores salvaguardas para os cidadãos. Naquela ocasião, constatou esta Corte que não existem mais dados pessoais insignificantes: isto é, todo tratamento de dados pessoais apresenta um potencial de risco intrínseco que demanda a implementação de mecanismos de proteção aos titulares para que possa se legitimar em uma sociedade democrática.
>
> Com aquela decisão, a proteção de dados no Brasil passou a proporcionar a garantia dos direitos inalienáveis do cidadão na era digital, posicionando-se na nossa ordem jurídica como instrumento para a consolidação da democracia e das liberdades. Hoje, a partir de seus dados pessoais, cidadãos podem ser analisados, avaliados, monitorados, discriminados e… controlados, além de

---

Procurador-Geral da República, sucessivamente, no prazo de cinco dias, submeter o processo diretamente ao Tribunal, que terá a faculdade de julgar definitivamente a ação".

> extirpados de sua autonomia e dignidade por frequentes decisões que afetam suas vidas serem tomadas a partir de seus dados, sem o devido processo e sem que tenham oportunidade de participação. É assim, aliás, que assevera a prof Laura Schertel Mendes em artigo publicado recentemente no jornal O Globo, no qual destaca como o poder informacional, que é derivado do controle sobre o uso da informação, pode ser malversado a prejuízo dos direitos e garantias fundamentais.[12]

A decisão foi proferida pelo STF em 15 de setembro de 2022, tendo ocorrido o julgamento conjunto da ADI n.º 6.649/DF com a ADPF n.º 695/DF, como analisaremos abaixo. O STF definiu critérios constitucionais relativos à atuação do Estado na coleta e no tratamento de dados dos cidadãos e no tocante aos parâmetros para compartilhamento de dados pessoais entre órgãos públicos e entre os entes estatais e os agentes privados.

1.2. *A ADPF nº 695/DF (o caso ABIN-Denatran)*

Em junho de 2020, o site jornalístico "Intercept Brasil" noticiou que a Agência Brasileira de Inteligência (ABIN) e o Serviço Federal de Processamento de Dados (Serpro) estabeleceram tratativas visando ao compartilhamento de dados dos mais de 76 milhões de brasileiros que possuíam Carteira Nacional de Habilitação – CNH naquela época (o equivalente a 36% da população total do país), originalmente coletados e armazenados pelo Departamento Nacional de Trânsito – Denatran .[13]

Os dados, que seriam atualizados mensalmente, incluíam incluem nomes, filiação, endereços, telefones, dados dos veículos e fotos de todo portador de CNH. Esses dados pessoais seriam extraídos do sistema "Renach", o Banco de Imagens do Registro Nacional de Condutores Habilitados, de responsabilidade do Denatran.

Em 9 de março de 2020, o compartilhamento de dados entre Denatran e ABIN foi formalizado por meio do Termo de Autorização nº 7/2020-A, autorizando

---

[12] DONEDA, Danilo. Sustentação oral na ADI n. 6649. **civilistica.com**, v. 11, n. 3, 25 dez. 2022, p. 2-3.
[13] DIAS, Tatiana; MARTINS, Rafael Moro. Documentos vazados mostram que ABIN pediu ao SERPRO dados e fotos de todas as CNHs do país. **Intercept Brasil,** 6 Jun. 2020. Disponível em: https://www.intercept.com.br/abin-carteira-motorista-serpro-vigilancia/. Acesso em: 20 set. 2023.

oficialmente o acesso da Agência à base de dados do Denatran. O documento previa, especificamente, "o acesso e a disponibilização eletrônica de dados dos sistemas e subsistemas informatizados do Departamento Nacional de Trânsito".

O principal fundamento que embasou o Termo de Autorização era o Decreto nº 10.046/2019, que instituiu o Cadastro Base do Cidadão; ou seja, o Decreto foi efetivamente utilizado como fundamento da legalidade do acordo entre ABIN e Serpro.

No dia 18 de junho de 2020, o Partido Socialista Brasileiro (PSB) ajuizou, no STF, a ADPF n.º 695/DF, questionando o compartilhamento dos dados pessoais entre o Serpro e a ABIN com lastro normativo no Decreto nº 10.046/2019.

A arguição de descumprimento de preceito fundamental, com pedido de liminar, requereu que fossem "reconhecidas e sanadas as graves e iminentes lesões e ameaça de lesões a preceitos fundamentais da Constituição Federal", decorrentes do alegado "compartilhamento de dados pessoais – quais sejam, os dados inerentes aos registros de carteiras de habilitação de mais de 76 milhões de brasileiros como nomes, filiação, endereços, telefones, dados dos veículos e fotos de todo portador de Carteira Nacional de Motorista – pelo Serviço Federal de processamento de Dados (Serpro) à Agência Brasileira de Inteligência (ABIN), com suposto lastro normativo no Decreto nº 10.046, de 9 de outubro de 2019, que traz normas e diretrizes para o compartilhamento de dados entre os órgãos e as entidades da administração pública federal direta, autárquica e fundacional e os demais Poderes da União".

O partido político autor da ADPF alegou que "o compartilhamento de volume avassalador e indiscriminado de dados pessoais com a Agência Brasileira de Inteligência viola frontal e inequivocamente o direito à liberdade e à dignidade da pessoa humana (art. 1º, III, e art. 5 º, *caput*), bem como, e especificamente, os direitos à privacidade, à proteção de dados pessoais e à autodeterminação informativa, preceitos fundamentais protegidos pela Constituição Federal (art. 5º, *caput* e incisos X e XII)" e sustentou, em síntese, que o "ato do poder público trazido a exame por esta Suprema Corte (i) viola os preceitos fundamentais da proteção da privacidade, bem como sua consequente garantia de proteção dos dados pessoais e de autodeterminação informativa dos cidadãos brasileiros (art. 5º, incisos X e XII da CF/88). Asseverou, ainda, que o compartilhamento (ii) não passa por crivo de

proporcionalidade ou de razoabilidade e (iii) nem possui base normativa que eventualmente lhe dê guarida. Finalmente, dada a absoluta ausência de clareza quanto à real finalidade - à luz das competências da Agência Brasileira de Inteligência - do tratamento dos dados transferidos de forma massiva e indiscriminada, (iv) põe em risco o basilar princípio democrático, fundante de nossa ordem constitucional, visto haver risco de vigilância massiva sem controle de cidadãs e cidadãos sem qualquer envolvimento com ações ou práticas ilegais".

Foram admitidos, na condição de *amicus curiae*, o Laboratório de Políticas Públicas e Internet LAPIN, a Associação dos Servidores da Agência Brasileira de Inteligência – ASBIN, a Associação Lawgorithm de Pesquisa em Inteligência Artificial, o Instituto Betal para Democracia e Internet – IBIDEM, o INTERVOZES – Coletivo Brasil de Comunicação Social e o Instituto Mais Cidadania.

Embora a União tenha prestado informações alegando inexistir qualquer violação aos preceitos constitucionais invocados, como resposta do governo ao ajuizamento da ADPF, *o Ministério da Infraestrutura, em 23 de junho de 2020, editou a Revogação do Termo de Autorização nº 7/2020-A.*

No dia 24 de junho de 2020, a liminar foi indeferida pelo Relator da ADPF n.º 695, Ministro Gilmar Mendes, devido à ausência do perigo da demora – uma vez que o acordo de compartilhamento fora revogado um dia antes da decisão. No entanto, o Ministro Gilmar Mendes trouxe em sua decisão considerações relevantes, tanto sobre a proteção de dados pessoais como um direito fundamental autônomo, quanto sobre o Decreto n.º 10.046/2019:

> Como amplamente analisado nesta decisão, o regime jurídico de compartilhamento de dados entre órgãos e instituições do Poder Público é matéria de extrema relevância para a proteção constitucional do direito constitucional à privacidade (art. 5º, caput e incisos X, da Constituição Federal), situando-se como garantia elementar de qualquer sociedade democrática contemporânea. Por esse motivo, é dever constitucional deste STF debruçar-se sobre a matéria, evitando-se que situações graves que colocam em risco a violação de preceitos fundamentais sejam perpetradas com suposto fundamento no Decreto nº. 10.046, de 9 de outubro de 2019. Destaca-se ainda

que a presente decisão não obsta a eventual análise de medida acauteladora relacionada a alegações de inconstitucionalidade deste ato normativo.[14]

1.3. *O Resultado do Julgamento Conjunto da ADI 6.649 e da ADPF 695*

O STF julgou parcialmente procedentes os pedidos formulados na ADI n.º 6.649 e na ADPF n.º 695 e deu interpretação conforme à Constituição ao Decreto n.º 10.046/2019, listando uma série de parâmetros que devem ser incorporados nas regras administrativas para o compartilhamento de dados na administração pública, conforme se extrai trecho do voto proferido pelo Min. Gilmar Mendes, ratificado pela maioria dos Ministros do STF, com exceção do Min. Edson Fachin, que votou pela declaração *in totum* da inconstitucionalidade do Decreto nº 10.046/2019, e dos Ministros André Mendonça e Nunes Marques, que divergiram em relação a alguns pontos do voto do Relator.

> 1. O compartilhamento de dados pessoais entre órgãos e entidades da Administração Pública, pressupõe: a) eleição de propósitos legítimos, específicos e explícitos para o tratamento de dados (art. 6º, inciso I, da Lei 13.709/2018); b) compatibilidade do tratamento com as finalidades informadas (art. 6º, inciso II); c) limitação do compartilhamento ao mínimo necessário para o atendimento da finalidade informada (art. 6º, inciso III); bem como o cumprimento integral dos requisitos, garantias e procedimentos estabelecidos na Lei Geral de Proteção de Dados, no que for compatível com o setor público.
> 2. O compartilhamento de dados pessoais entre órgãos públicos pressupõe rigorosa observância do art. 23, inciso I, da Lei 13.709/2018, que determina seja dada a devida publicidade às hipóteses em que cada entidade governamental compartilha ou tem acesso a banco de dados pessoais, "fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos".

---

[14] BRASIL. Supremo Tribunal Federal. Tribunal Pleno. **Ação de Descumprimento de Preceito Fundamental nº 695 Distrito Federal**. Relator: Ministro Gilmar Mendes. Decisão Monocrática. Brasília, 24.6.2020.

3. O acesso de órgãos e entidades governamentais ao Cadastro Base do Cidadão fica condicionado ao atendimento integral das diretrizes acima arroladas, cabendo ao Comitê Central de Governança de Dados, no exercício das competências aludidas nos arts. 21, incisos VI, VII e VIII do Decreto 10.046/2019:
3.1. prever mecanismos rigorosos de controle de acesso ao Cadastro Base do Cidadão, o qual será limitado a órgãos e entidades que comprovarem real necessidade de acesso aos dados pessoais nele reunidos. Nesse sentido, a permissão de acesso somente poderá ser concedida para o alcance de propósitos legítimos, específicos e explícitos, sendo limitada a informações que sejam indispensáveis ao atendimento do interesse público, nos termos do art. 7º, inciso III, e art. 23, caput e inciso I, da Lei 13.709/2018;
3.2. justificar prévia e minudentemente, à luz dos postulados da proporcionalidade, da razoabilidade e dos princípios gerais de proteção da LGPD, tanto a necessidade de inclusão de novos dados pessoais na base integradora (art. 21, inciso VII) como a escolha das bases temáticas que comporão o Cadastro Base do Cidadão (art. 21, inciso VIII).
3.3. instituir medidas de segurança compatíveis com os princípios de proteção da LGPD, em especial a criação de sistema eletrônico de registro de acesso, para efeito de responsabilização em caso de abuso.
4. O compartilhamento de informações pessoais em atividades de inteligência observará o disposto em legislação específica e os parâmetros fixados no julgamento da ADI 6.529, quais sejam: (i) adoção de medidas proporcionais e estritamente necessárias ao atendimento do interesse público; (ii) instauração de procedimento administrativo formal, acompanhado de prévia e exaustiva motivação, para permitir o controle de legalidade pelo Poder Judiciário; (iii) utilização de sistemas eletrônicos de segurança e de registro de acesso, inclusive para efeito de responsabilização em caso de abuso; e (iv) observância dos princípios gerais de proteção e dos direitos do titular previstos na LGPD, no que for compatível com o exercício dessa função estatal.
5. O tratamento de dados pessoais promovido por órgãos públicos ao arrepio dos parâmetros legais e constitucionais (ingerência) importará a responsabilidade civil do Estado pelos danos suportados pelos particulares, na forma dos arts. 42 e seguintes da Lei 13.709/2018, associada ao exercício do direito de regresso contra os servidores e agentes políticos responsáveis pelo ato ilícito, em caso de dolo ou culpa.

> 6. A transgressão dolosa ao dever de publicidade estabelecido no art. 23, inciso I, da LGPD, fora das hipóteses constitucionais de sigilo, importará a responsabilização do agente estatal por ato de improbidade administrativa, nos termos do art. 11, inciso IV, da Lei 8.429/92, sem prejuízo da aplicação das sanções disciplinares previstas nos estatutos dos servidores públicos federais, municipais e estaduais.[15]

Finalmente, o Tribunal declarou, com efeito *pro futuro*, **a inconstitucionalidade do art. 22 do Decreto n.º 10.046/19,** preservando a atual estrutura do Comitê Central de Governança de Dados pelo prazo de 60 dias, a contar da data de publicação da ata de julgamento, a fim de garantir ao Chefe do Poder Executivo prazo hábil para (i) atribuir ao órgão um perfil independente e plural, aberto à participação efetiva de representantes de outras instituições democráticas; e (ii) conferir aos seus integrantes garantias mínimas contra influências indevidas.

Em cumprimento à decisão, foram editados posteriormente o Decreto n.º 11.266/2022, com a nova conformação do Comitê Central de Governança de Dados, e o Decreto n.º 11.574/2023, com alterações para aperfeiçoamento do texto original.

2. Comentários sobre a decisão

O Decreto n.º 10.046/2019 foi erigido com embasamento no paradigma anterior à decisão histórica do STF na ADI 6.387 e à Emenda Constitucional 115/2022, que inseriu expressamente o direito à proteção de dados pessoais no rol de direitos fundamentais do art. 5º da Constituição Federal. Nesse paradigma anterior, conferia-se *tutela constitucional* apenas à *privacidade e ao sigilo "da comunicação de dados";* ou seja, *não se reconhecia a tutela constitucional dos "dados em si mesmos"*.[16]

---

[15] BRASIL. Supremo Tribunal Federal. Tribunal Pleno. **Ação Direta de Inconstitucionalidade 6.649 Distrito Federal**. Relator: Ministro Gilmar Mendes. Brasília, 15 set. 2022.

[16] Nesse sentido, o antigo paradigma da Corte Constitucional era na direção de que a tutela constitucional se destinava apenas à comunicação dos dados (ao sigilo das comunicações) e não aos dados propriamente ditos. Para maiores detalhes, cf. BRASIL. Supremo Tribunal Federal. Tribunal Pleno. **Recurso Extraordinário 418.416-8 Santa Catarina**. Relatora: Ministro Sepúlveda Pertence. Brasília, 10 maio 2006; BRASIL. Supremo Tribunal Federal. Segunda Turma. **Habeas Corpus 91.867 Pará.** Relator: Ministro Gilmar Mendes. Brasília, 24 abril 2012.

A ADI n.º 6.649 questionou a constitucionalidade do Decreto 10.046/2019, que criou o Cadastro Base do Cidadão e o Comitê Central de Governança e previu medidas que supostamente facilitariam o acesso dos brasileiros a serviços públicos federais digitais. Entretanto, na prática – como demonstram os fatos narrados na ADPF n.º 695 (Caso ABIN-Denatran) – o Decreto n.º 10.046 estava sendo utilizado para a criação de uma ferramenta de vigilância estatal poderosa e fora da sistemática prevista na LGPD, com a ampliação da coleta de dados sensíveis, através de técnicas de biometria comportamental – incorporadas por tecnologias de monitoramento – e para um possível controle político intenso dos cidadãos, típico de regimes totalitários.

Como descrevemos no tópico 1.2 *supra*, o convênio ABIN/Serpro, celebrado através do Termo de Autorização nº 7/2020-A com fundamento no Decreto 10.046/2019, violou os direitos fundamentais da privacidade, da proteção dos dados pessoais e de autodeterminação informativa dos cidadãos brasileiros (art. 5º, incisos X, XII e LXXII da CF/88). Tal ato administrativo não passaria pelo crivo de proporcionalidade ou de razoabilidade e era patente a absoluta ausência de clareza quanto à real finalidade do convênio – à luz das competências da Agência Brasileira de Inteligência. *O tratamento dos dados transferidos de forma massiva e indiscriminada colocava em risco o basilar princípio democrático, fundante de nossa ordem constitucional, tendo em vista a operação estatal de vigilância massiva de 1/3 da população brasileira* – e a esmagadora maioria dos cidadãos em qualquer envolvimento com práticas ilegais ou ameaçadoras ao Estado brasileiro.

Analisando os fatos narrados na ADPF 695, o STF reconheceu os efeitos maléficos do Decreto 10.046/2019 e destacou que este não se harmonizava com a decisão proferida na ADI n.º 6.387, na qual foi superado antigo paradigma da própria Corte, com o reconhecimento do direito à proteção de dados como um novo direito fundamental, destacado e independente do direito à privacidade, com a identificação de uma série de liberdades individuais, atreladas ao direito à proteção de dados pessoais, que não são abraçadas pelo direito à privacidade, isto é, na concepção da

privacidade como uma garantia de abstenção do Estado na esfera privada individual.[17]

O caso ABIN-Denatran foi essencial para evidenciar que, nos termos dispostos pelo Decreto n.º 10.046/2019, o Cadastro Base do Cidadão poderia se transformar numa ferramenta de vigilância estatal extremamente poderosa, que incluía informações pessoais básicas, mas também dados laborais e biométricos, como "características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar" (art. 2º, II, do Decreto n.º 10.046/2019).

Além disso, a estrutura de governança do Decreto n.º 10.046/2019, com o Comitê Central de Governança de Dados, não era recomendável, haja vista que tal Comitê Central não seria composto pela Autoridade Nacional de Proteção de Dados tampouco por representantes de empresas e de entidades da sociedade civil. Trata-se de uma estrutura jurídica que contrariava aquilo que as leis sobre a relação entre direito e tecnologia exigem em relação à governança. Tanto o Marco Civil da Internet (Lei nº 12.485/2014) quanto a LGPD apontam isso ao exaltar a participação de estruturas multissetoriais, como o Comitê Gestor da Internet (CGI.Br) e o Conselho Nacional de Proteção de Dados (CNPD).

A criação de tais normas através do Decreto 10.046/2019 seguia na contramão de tudo o que se encaminhou na última década em relação à discussão político-jurídica da proteção de dados, aos princípios da LGPD e à histórica decisão do STF: a implantação de um super cadastro com concentração de dados e enormes riscos de segurança; o uso e compartilhamento de dados pessoais sem consentimento e sem finalidade expressa; a total ausência de discussão pública prévia envolvendo a sociedade civil, os empresários e os órgãos multissetoriais (como o Comitê Gestor da Internet). Além disso, não foram lançadas campanhas de

---

[17] Vale ressaltar que, ao exame do referendo das medidas cautelares nas ADIs 6.387/DF, 6.388/DF, 6.389/DF, 6.390/DF e 6.393/DF, o Plenário do Supremo Tribunal Federal confirmou a suspensão da Medida Provisória 954/2020 que determinava o compartilhamento, com o IBGE, de dados dos usuários de serviço telefônico comutado fixo e de serviço móvel pessoal.

conscientização e de alerta à população em relação às novas políticas públicas que estavam sendo implantadas.

A grandiosidade da empreitada gerava fundadas suspeitas de riscos de vazamentos de dados pessoais, visto que essa sistemática infralegal do decreto disciplinava a centralização de 51 bases de cadastro nacionais (CPF, Renavam, CNPJ, FGTS, Folha Salarial do Seguro-Desemprego, Sisu, ProUni, Fies, Prontuário Eletrônico dos Pacientes do SUS, etc.), além das novas bases (Base Integradora e Base Temática) compostas por atributos biográficos e por atributos biométricos de todos os brasileiros.

Em resumo, existiam inúmeros aspectos preocupantes que impunham o questionamento da constitucionalidade do Decreto n.º 10.046/2019: o não atendimento aos princípios de proteção de dados pessoais estabelecidos pela LGPD e pelo ordenamento constitucional; a facilitação de programas futuros para celebração de convênios de acessos a empresas privadas que acessariam essas informações do cadastro centralizado; problemas sérios de governança, posto que o Comitê Central de Governança previsto no Decreto n.º 10.046/2019 composto apenas por órgãos do governo federal, sem qualquer participação de entidades da sociedade civil; a ausência da Autoridade Nacional de Proteção de Dados nas decisões e na supervisão do Comitê Central de Governança, em descompasso com as normas da LGPD e criando a possibilidade de decisões contraditórias de órgãos governamentais superpostos, decisões estas que poderão ser extremamente prejudiciais para os titulares de dados pessoais.

A decisão proferida pelo STF, em 15 de setembro de 2022, sob a Relatoria do Ministro Gilmar Mendes, no âmbito da ADI n.º 6.649/DF, julgada conjuntamente com a ADPF 695/DF, é um *leading case* que definiu critérios constitucionais relativos à atuação do Estado na coleta e no tratamento de dados dos cidadãos e no tocante aos parâmetros para compartilhamento de dados pessoais entre órgãos públicos e entre os entes estatais e os agentes privados.

É importante destacar que a maioria dos Ministros do STF acompanhou a solução adotada pelo Relator de aplicação da técnica decisória da interpretação conforme à Constituição. Esta solução foi adotada porque a Corte considerou que a declaração da inconstitucionalidade do Decreto n.º 10.046/2019, na sua

integralidade, acabaria por "destituir os órgãos do Poder Executivo de normas operacionais necessárias ao compartilhamento de dados no interesse da eficiente prestação de serviços públicos". Além disso, destacou o Ministro Gilmar Mendes, o efeito repristinatório do Decreto n.º 8.789/2016 (revogado pelo Decreto 10.046) seria ainda mais nocivo para a privacidade e causaria ainda mais insegurança e instabilidade:

> Nesse sentido, a extirpação pura e simples da norma impugnada poderia acarretar, fundamentalmente, a formação de vácuo regulamentar numa área relevante e sensível para o gestor público, com impactos nocivos para a eficiência e segurança da atividade administrativa.
> Em um outro cenário, caso se entenda pela repristinação do Decreto 8.789/2016, revogado pelo atual regulamento, o resultado seria ainda mais nocivo à proteção de privacidade. A norma anterior estabelecia que os dados cadastrais sob gestão dos órgãos públicos federais seriam "compartilhados entre as bases de dados oficiais, preferencialmente de forma automática, para evitar novas exigências de apresentação de documentos e informações e possibilitar a atualização permanente e simultânea dos dados".
> Dado o obsoletismo do texto anterior, é lícito concluir que o efeito repristinatório da declaração de inconstitucionalidade causaria ainda mais insegurança e instabilidade, na medida em que os dispositivos revogados não apenas impunham o compartilhamento automático de informações cadastrais entre todos os órgãos públicos federais, como também silenciavam completamente a respeito da adoção de salvaguardas institucionais para proteção de dados pessoais. Evidencia-se, a não mais poder, a necessidade de adoção da técnica decisória intermediária da interpretação conforme à Constituição.[18]

No tocante ao Comitê Geral de Governança de Dados, a decisão apontou as distorções na composição do Comitê Geral de Governança de Dados, e foi declarada, com efeito futuro, a inconstitucionalidade do art. 22 do Decreto 10.046/2019, a fim de que, no prazo de 60 dias, o poder público atribuísse ao referido órgão perfil

[18] BRASIL. Supremo Tribunal Federal. Tribunal Pleno. **Ação Direta de Inconstitucionalidade 6.649 Distrito Federal**. Relator: Ministro Gilmar Mendes. Brasília, 15 set. 2022.

independente e plural, bem como conferisse a seus integrantes garantias mínimas contra influências indevidas.

Na esfera da segurança pública, das atividades de inteligência do Estado e de persecução penal, a decisão do STF foi decisiva para sedimentar os contornos do direito fundamental à proteção de dados, em face das exceções previstas no art. 4º, inciso III, da LGPD (tratamento de dados em atividades de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão penais), que "deverão ser regidas por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei" (§ 1º do art. 4º da LGPD). *Lamentavelmente, essa legislação específica ainda não foi editada pelo Congresso Nacional, em que pese o excelente trabalho desenvolvido pela Comissão de Juristas que elaborou o anteprojeto de LGPD Penal e da qual participou Danilo Doneda.*

O acórdão da ADI n.º 6.649 (e da ADPF 695) está conectado à decisão proferida na ADI n.º 6.529/DF[19] (Caso "ABIN Paralela"), de Relatoria da Ministra Cármen Lúcia, haja vista que o item 4 da decisão proferida na ADI 6.649 se reporta aos parâmetros fixados no julgamento da ADI n.º 6.529 em relação às atividades de inteligência do Estado:

> 4. O compartilhamento de informações pessoais em atividades de inteligência observará o disposto em legislação específica e os parâmetros fixados no julgamento da ADI 6.529, Rel. Min. Cármen Lúcia, quais sejam: (i) adoção de medidas proporcionais e estritamente necessárias ao atendimento do interesse público; (ii) instauração de procedimento administrativo formal, acompanhado de prévia e exaustiva motivação, para permitir o controle de legalidade pelo Poder Judiciário; (iii) utilização de sistemas eletrônicos de segurança e de registro de acesso, inclusive para efeito de responsabilização em caso de abuso; e (iv)

[19] BRASIL. Supremo Tribunal Federal. Tribunal Pleno. **Ação Direta de Inconstitucionalidade 6.529 Distrito Federal**. Relator: Cármen Lúcia. Brasília, 11 out. 2021.

> observância dos princípios gerais de proteção e dos direitos do titular previstos na LGPD, no que for compatível com o exercício dessa função estatal.[20]

Como afirma Laura Schertel Mendes, o poder informacional do Estado diz respeito ao "poder oriundo do tratamento de informações e do conhecimento gerado a partir delas. Poder que, se usado para alcançar os objetivos legais do Estado, de forma supervisionada, transparente e procedimentalizada, é considerado legítimo".[21]

Os casos do Cadastro Base do Cidadão, da ABIN-Denatran e da "ABIN Paralela" demonstram o quanto é **perigosa a instrumentalização do poder informacional pelo Estado** "quando usado para subjugar indivíduos por meio da vigilância ininterrupta e sorrateira, bem como para a tomada de decisões sem o devido processo legal e sem oportunidades de participação do cidadão, é a própria subversão do Estado de Direito (...)".[22]

Em todo o mundo, as autoridades públicas utilizam cada vez mais a inteligência artificial e novas tecnologias para executar serviços públicos, configurando-se um cenário que a Organização das Nações Unidas chama de "*digital welfare states*" – Estados de bem-estar social digital. [23] Muitos pesquisadores apontam que, embora os governos argumentem que as novas tecnologias tornam os seus serviços mais eficientes e rentáveis, aumentam as preocupações com a vigilância dos cidadãos. [24]

Os desafios de harmonizar os objetivos do Estado com os interesses legítimos dos titulares dos dados pessoais são crescentes com o uso de novas tecnologias de

---

[20] BRASIL. Supremo Tribunal Federal. Tribunal Pleno. **Ação Direta de Inconstitucionalidade 6.649 Distrito Federal**. Relator: Ministro Gilmar Mendes. Brasília, 15 set. 2019.

[21] MENDES, Laura Schertel. Democracia, poder informacional e vigilância: limites constitucionais ao compartilhamento de dados pessoais na Administração Pública. **O GLOBO**, 13 ago. 2022. Disponível em: https://oglobo.globo.com/blogs/fumus-boni-iuris/post/2022/08/laura-schertel-democracia-poder-informacional-e-vigilancia.ghtml. Acesso em: 20 set. 2023.

[22] MENDES, Laura Schertel. Democracia, poder informacional e vigilância: limites constitucionais ao compartilhamento de dados pessoais na Administração Pública. **O GLOBO**, 13 ago. 2022. Disponível em: https://oglobo.globo.com/blogs/fumus-boni-iuris/post/2022/08/laura-schertel-democracia-poder-informacional-e-vigilancia.ghtml. Acesso em: 20 set. 2023.

[23] UNITED NATIONS. **A/74/93**: Digital welfare states and human rights – Report of the Special Rapporteur on extreme poverty and human rights. Nova York: 2019. Disponível em: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/312/13/PDF/N1931213.pdf?OpenElement: Acesso em: 20 set. 2023.

[24] BEKKER, Sonja. **Fundamental Rights in Digital Welfare States**: the case of SyRI in the Netherlands. Netherlands: Netherlands Yearbook of International Law 2019, 2021, p. 289, tradução livre.

informação e comunicação e sistemas de inteligência artificial. Neste sentido, compete ao Poder Público o desafio de conciliar os "princípios tradicionalmente aplicáveis à Administração Pública e aqueles contidos na própria LGPD, sem que se determine a precedência *prima facie* de um interesse público abstratamente caracterizado e reconhecendo também a importância da proteção de dados pessoais para além da sua dimensão individual".[25]

A implementação de tecnologias algorítmicas no processamento de dados pessoais aumentou as preocupações dos indivíduos, que estão sujeitos a formas de controle e vigilância, com ameaças ao próprio regime democrático.[26] As ferramentas de inteligência artificial que usam dados pessoais coletados em massa multiplicaram-se em praticamente todos os campos da atividade humana e é essencial identificar e mitigar os seus impactos. Nesse sentido, vale transcrever a advertência contida em trecho do voto de Ministro Gilmar Mendes na ADI 6.387 acerca da proteção dos valores estruturantes da nossa democracia constitucional:

> Todo esse contexto nos indica que decisões críticas para o Estado de Direito estão sendo cada vez mais substituídas por mecanismos automatizados. Em outras palavras, de forma bem direta: vivemos na era das escolhas de Sofia automatizadas. Independente do acerto ou desacerto dessas decisões automatizadas, é inequívoco que a proteção dos valores estruturante da nossa democracia constitucional requer que o Direito atribua elementos de transparência e controle que preservem o exercício da cidadania. É por isso que, para muito além do mero debate sobre o sigilo comunicacional, este Tribunal deve reconhecer que a disciplina jurídica do processamento e da utilização da informação acaba por afetar o sistema de proteção de garantias individuais como um todo.[27]

---

[25] WIMMER, Miriam. Regime Jurídico do Tratamento de Dados Pessoais pelo Poder Público. In: DONEDA, Danilo; MENDES, Laura Schertel; RODRIGUES JR, Otávio Luiz; SARLET, Ingo Wolfgang (coord.), BIONI, Bruno (Coord. Executivo). **Tratado de proteção de dados pessoais**. 1. ed. Rio de Janeiro: Forense, 2021, 278.

[26] DE GREGORIO, Giovanni. **Digital constitutionalism in Europe:** reframing rights and powers in the algorithmic society. Cambridge, Reino Unido: Cambridge University Press, 2022, p. 271.

[27] BRASIL. Supremo Tribunal Federal. Tribunal Pleno. **Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6.387 Distrito Federal**. Relatora: Ministra Rosa Weber. Brasília, 7 maio 2020.

Considerações finais

Segundo Stefano Rodotà, "a proteção de dados constitui não apenas um direito fundamental entre outros: é o mais expressivo da condição humana contemporânea". [28] A proteção de dados pessoais é um direito fundamental autônomo que não se confunde com a privacidade e com outros direitos fundamentais; a proteção de dados tem um núcleo essencial e possui um âmbito próprio e reservado de proteção. Ainda que se possa afirmar que a proteção de dados pessoais tem "na autodeterminação informativa o seu eixo estruturante", ela possui "um alcance mais alargado e multidimensional, exigindo também o reconhecimento e concretização de um princípio da separação informacional de poderes".[29]

No julgamento da ADI n.º 6.649, ficou evidente a tensão entre a defesa do interesse público – que busca a eficiência e a digitalização dos serviços públicos – e a privacidade e a proteção de dados pessoais. As justificativas trazidas pela defesa do governo federal brasileiro de que o Decreto n.º 10.046/2019 atribui "maior eficiência na prestação de serviços públicos" e "implementa diretriz de desburocratização" mascaravam os perigos de que, em nome dos benefícios do governo digital, estavam sendo implementados mecanismos que violavam direitos e garantias fundamentais, como ocorreu no caso ABIN-Denatran. Trata-se de um *trade-off* inaceitável e inconstitucional. A atividade eficiente da Administração Pública e o interesse tutelado pelo Estado devem "ser compreendidos no contexto de um conjunto mais amplo de princípios e com elementos integrantes do compromisso que o Estado deve ter com a democracia e com a concretização de direitos fundamentais".[30]

---

[28] RODOTÀ, Stefano. **A vida na sociedade de vigilância**. MORAES, Maria Celina Bodin de (org.). Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 26.

[29] SARLET, Ingo Wolfgang; SALES SARLET, Gabrielle. **Separação informacional de poderes no direito constitucional brasileiro**. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2022, p. 26. Disponível em: file:///C:/Users/msgar/Downloads/DataPrivacy.-Separacao-Informacional-de-Poderes.-2022.pdf. Acesso em: 3 out. 2023.

[30] WIMMER, Miriam. Regime Jurídico do Tratamento de Dados Pessoais pelo Poder Público. In: DONEDA, Danilo; MENDES, Laura Schertel; RODRIGUES JR, Otávio Luiz; SARLET, Ingo Wolfgang (coord.), BIONI, Bruno (Coord. Executivo). **Tratado de proteção de dados pessoais**. 1. ed. Rio de Janeiro: Forense, 2021, 278.

O julgamento da ADI n.º 6.649 e da ADPF n.º 695 abordou preocupações em relação à separação informacional de poderes, ao "tecnoautoritarismo" e ao uso de técnicas de vigilância tecnológica em massa pelo Estado, que permitem a coleta de imensas quantidades de dados pessoais e metadados sem o conhecimento ou consentimento dos indivíduos, podendo minar os seus direitos fundamentais como a privacidade, a proteção de dados pessoais e a liberdade de expressão e associação.

Diante dos desafios enfrentados para a consecução do princípio da separação informacional de poderes no direito constitucional brasileiro, a decisão do STF adotou critérios interpretativos para a aplicação desse princípio fundamental em face das novas tecnologias de informação e comunicação e do crescente compartilhamento de dados pessoais em poder do Estado brasileiro, garantindo critérios e parâmetros de adequação, proporcionalidade e necessidade, com bases legais e finalidades apropriadas, bem como medidas de segurança e transparência que garantam a proteção de dados dos cidadãos, bem como a motivação das decisões que envolvam todas as formas de tratamento de dados.

Reiteramos que os riscos apontados nas ações analisadas ainda levantam discussões sobre vigilância estatal, separação informacional de poderes, devido processo informacional e utilização de tecnologias da informação que podem ameaçar ou violar direitos fundamentais. Neste sentido, a título de crítica, destacamos que o Decreto n.º 10.046/2019, apesar das recentes modificações feitas através dos Decretos n.ºs 11.266/2022[31] e 11.574/2023[32] em cumprimento à decisão do STF na ADI 6.649, ***ainda necessita de novos aperfeiçoamentos, haja vista que a técnica de intepretação conforme adotada pela Corte impôs um conjunto de comandos muito complexos, amplos e procedimentais, que exigiriam, na prática, a***

[31] BRASIL. **Decreto n.º 11.266, de 25 de novembro de 2022**. Altera o Decreto nº 10.046, de 9 de outubro de 2019, que dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Presidência da República. Brasília, DF.

[32] BRASIL. **Decreto n.º 11.574, de 20 de junho de 2023**. Altera o Decreto nº 10.046, de 9 de outubro de 2019, que dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Presidência da República. Brasília, DF.

***elaboração de um novo decreto, o que gerará, certamente, novas controvérsias e debates*.**

Além disso, o ***atraso na edição da legislação infraconstitucional de proteção de dados que regulamente as exceções previstas no art. 4º, inciso III, da LGPD*** (tratamento de dados em atividades de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão penais) é ***extremamente preocupante para o âmbito de proteção dos direitos fundamentais à privacidade e à proteção de dados pessoais***, visto que o princípio da separação informacional de poderes exige a regulamentação infraconstitucional pautada pela repartição de competências e guiada pela finalidade da coleta e tratamento dos dados e por parâmetros de adequação, proporcionalidade e necessidade, com bases legais e finalidades apropriadas, bem como medidas de segurança e transparência que garantam a proteção dos direitos dos cidadãos.

Em face da dimensão objetiva do direito à proteção de dados pessoais, compete ao Poder Público atuar de maneira mais firme e interventiva, com a finalidade de assegurar a efetividade e eficácia do direito fundamental em questão, notadamente para salvaguardá-lo da indevida ingerência proveniente do próprio Estado e de agressões oriundas de particulares.

Nessa ordem de ideias, ***compete ao Estado legislar e criar a normativa necessária em termos da proteção de dados na área penal, a fim de sejam normatizados os procedimentos e a mitigados os efeitos das restrições ao direito fundamental à proteção de dados pessoais e à privacidade quando ocorre a atuação estatal nas atividades de segurança pública, inteligência e persecução penal.***

Por derradeiro, enaltecemos o imenso legado de Danilo Doneda na construção do marco normativo da privacidade e da proteção de dados pessoais, tanto na esfera legislativa, quanto no campo doutrinário e na jurisdição constitucional. Danilo nos deixou um legado permanente e continuará sendo inspiração e motivação para a luta pela cidadania e pelo exercício dos direitos e liberdades fundamentais.

Referências

BEKKER, Sonja. **Fundamental Rights in Digital Welfare States**: the case of SyRI in the Netherlands. Netherlands: Netherlands Yearbook of International Law 2019, 2021.

BRASIL. **Decreto n.º 8.789, de 29 de junho de 2016**. Dispõe sobre o compartilhamento de bases de dados na administração pública federal. Presidência. Presidência da República, Brasília, DF. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8789.htm. Acesso em: 4 out. 2023.

BRASIL. **Decreto n.º 10.046, de 9 outubro 2019**. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Presidência da República, Brasília, DF. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 4 out. 2023.

BRASIL. Ministério do Planejamento, Desenvolvimento e Gestão. Secretaria de Tecnologia da Informação. **Portaria n.º 58, de 23 de dezembro de 2016**. Dispõe sobre procedimentos complementares para o compartilhamento de bases de dados oficiais entre órgãos e entidades da administração pública federal direta e indireta e as demais entidades controladas direta ou indiretamente pela União. Brasília, DF. Disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/portarias-federais/portaria-no-58-de-23-de-dezembro-de-2016. Acesso em: 4 out. 2023.

BRASIL. **Decreto n. 10.047, de 9 outubro 2019**. Dispõe sobre a governança do Cadastro Nacional de Informações Sociais e institui o programa Observatório de Previdência e Informações, no âmbito do Cadastro Nacional de Informações Sociais. Presidência da República, Brasília, DF. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d10047.htm. Acesso em 4 out. 2023.

BRASIL. Supremo Tribunal Federal. Segunda Turma. **Habeas Corpus 91.867 Pará**. Relator: Ministro Gilmar Mendes. Brasília, 24 abril 2012.

BRASIL. Supremo Tribunal Federal. Tribunal Pleno. **Ação de Descumprimento de Preceito Fundamental nº 695 Distrito Federal**. Relator: Ministro Gilmar Mendes. Decisão Monocrática. Brasília, 24.6.2020.

BRASIL. Supremo Tribunal Federal. Tribunal Pleno. **Ação Direta de Inconstitucionalidade 6.529 Distrito Federal**. Relator: Cármen Lúcia. Brasília, 11 out. 2021.

BRASIL. Supremo Tribunal Federal. Tribunal Pleno. **Ação Direta de Inconstitucionalidade 6.649 Distrito Federal**. Relator: Ministro Gilmar Mendes. Brasília, 15 set. 2022.

BRASIL. Supremo Tribunal Federal. Tribunal Pleno. **Recurso Extraordinário 418.416-8 Santa Catarina**. Relatora: Ministro Sepúlveda Pertence. Brasília, 10 maio 2006.
BRASIL. Supremo Tribunal Federal. Tribunal Pleno. **Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6.387 Distrito Federal**. Relatora: Ministra Rosa Weber. Brasília, 7 maio 2020.

DE GREGORIO, Giovanni. **Digital constitutionalism in Europe:** reframing rights and powers in the algorithmic society. Cambridge, Reino Unido: Cambridge University Press, 2022.

DIAS, Tatiana; MARTINS, Rafael Moro. Documentos vazados mostram que ABIN pediu ao SERPRO dados e fotos de todas as CNHs do país. **Intercept Brasil,** 6 Jun. 2020. Disponível em: https://www.intercept.com.br/abin-carteira-motorista-serpro-vigilancia/. Acesso em: 20 set. 2023.

DONEDA, Danilo. Sustentação oral na ADI n. 6649. **civilistica.com**, v. 11, n. 3, 25 dez. 2022.

FERREIRA, Lucia Maria Teixeira. Parecer sobre a legalidade dos Decretos 10.046/2019 e 10.047/2019 em face das normas que disciplinam os direitos fundamentais à proteção de dados e à privacidade no ordenamento jurídico brasileiro. **Revista do Ministério Público do Estado do Rio de Janeiro**. n. 75, p. 258-259, jan./mar 2020.

MENDES, Laura Schertel. Autodeterminação informativa: a história de um conceito. **Pensar**, Fortaleza, v. 25, n. 4, p. 1-18, out./dez. 2020.

MENDES, Laura Schertel. Democracia, poder informacional e vigilância: limites constitucionais ao compartilhamento de dados pessoais na Administração Pública. **O GLOBO**, 13 ago. 2022. Disponível em: https://oglobo.globo.com/blogs/fumus-boni-iuris/post/2022/08/laura-schertel-democracia-poder-informacional-e-vigilancia.ghtml. Acesso em: 20 set. 2023.

RODOTÀ, Stefano. **A vida na sociedade de vigilância**. MORAES, Maria Celina Bodin de (org.). Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SARLET, Ingo Wolfgang; SALES SARLET, Gabrielle. **Separação informacional de poderes no direito constitucional brasileiro**. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2022. Disponível em: file:///C:/Users/msgar/Downloads/DataPrivacy.-Separacao-Informacional-de-Poderes.-2022.pdf. Acesso em: 3 out. 2023.

UNITED NATIONS. **A/74/93**: Digital welfare states and human rights – Report of the Special Rapporteur on extreme poverty and human rights. Nova York: 2019. Disponível em: https://documents-dds-

ny.un.org/doc/UNDOC/GEN/N19/312/13/PDF/N1931213.pdf?OpenElement: Acesso em: 20 set. 2023.
WIMMER, Miriam. Regime Jurídico do Tratamento de Dados Pessoais pelo Poder Público. In: DONEDA, Danilo; MENDES, Laura Schertel; RODRIGUES JR, Otávio Luiz; SARLET, Ingo Wolfgang (coord.), BIONI, Bruno (Coord. Executivo). **Tratado de proteção de dados pessoais**. 1. ed. Rio de Janeiro: Forense, 2021.

8. O PAPEL DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS – ANPD - NA PROTEÇÃO DO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS

 https://doi.org/10.36592/9786554600798-08

Melissa Barrioni e Oliveira[1]

Leide Jane Macedo da Silva[2]

RESUMO

Neste estudo, propomos uma abordagem ao papel da Autoridade Nacional de Proteção de Dados na proteção do direito fundamental à privacidade e à proteção de dados, considerando as atividades desenvolvidas pela autoridade e os desafios gerados pela falta de controle efetivo da sociedade e diante do avanço digital. A Autoridade tem a atribuição de fiscalizar e zelar pela proteção dos dados pessoais, assegurar a observância de segredos comerciais e industriais e punir eventuais descumprimentos à legislação e ainda, possui um papel "educador" e "fomentador" da cultura e na conscientização da proteção de dados. Na esteira de uma almejada garantia do direito à proteção de dados, buscaremos estudar o tema partindo de legislações, regulamentos, artigos e doutrinas. Em um cenário muito novo, desafiador e de extrema dificuldade na difusão da cultura e conscientização ao tema, restará abordado a importância do papel educacional e regulatório da Autoridade.
Palavras-chave: Autoridade Nacional de Proteção de Dados. Proteção de dados pessoais. Privacidade. Legislação. Conscientização.

1. Introdução

Na era digital em constante evolução, a proteção do direito fundamental à privacidade tornou-se uma preocupação premente em todo o mundo. Abordaremos os princípios ligados à proteção dos dados pessoais, uma vez que os princípios

[1] Presidente da Comissão de Proteção de Dados da OAB/MG - triênio 2022/2024. Membro Consultora da Comissão Especial de Proteção de Dados do CFOAB. Professora e Coordenadora da Pós-graduação em de Proteção de Dados e Privacidade da ESA/MG e CEDIN. Palestrante. Especializada em Compliance e LGPD. Partner e Co-founder da BSS Consult. Pós-Graduada em Direito do Trabalho e Processo do Trabalho pelo CAD (Centro de Atualização em Direito) e FUMEC/MG. Pós-Graduada em Docência com Ênfase em Educação Jurídica pela Universidade Arnaldo.

[2] Advogada na área de Direito e Tecnologia e Empresarial. Data Protection Officer. Especialista em Direito e Tecnologia, Proteção de Dados para o setor público e privado e Cibersegurança. Professora de Especialização PUC Minas e cursos voltados para administração pública no IDCT - Instituto de Defesa da Cidadania e da Transparência. Diretora do Núcleo de Pesquisa e Extensão da Comissão de Proteção de Dados da OAB/MG.

fundamentais que orientam a proteção de dados pessoais representam a espinha dorsal das legislações e tratados voltados para a preservação da privacidade em um mundo cada vez mais digital.

O tratamento autônomo da proteção de dados pessoais é uma tendência que hoje está firmemente enraizada em diversos ordenamentos jurídicos. Isso representa uma mudança notável na forma como encaramos a privacidade e a proteção dos dados pessoais. O que inicialmente parecia ser uma resposta pontual a desafios tecnológicos específicos evoluiu para se tornar um direito fundamental à proteção de dados, sendo desenvolvido uma série de legislações sobre o tema.

Evidenciamos a dificuldade de controle do uso dos dados na era digital em constante evolução, situação pela qual exige um compromisso constante com a ética e a segurança por parte de todos os envolvidos.

Nesse contexto, a Autoridade Nacional de Proteção de Dados (ANPD) emerge como uma figura de extrema relevância. Neste estudo, faremos uma abordagem ao papel desempenhado pela ANPD na garantia da proteção desse direito fundamental tão essencial pelo cumprimento da Lei Geral de Proteção de Dados (LGPD). Analisamos as atividades que norteiam seu funcionamento, suas atribuições, as leis que a respaldam e os desafios significativos que ela enfrenta, bem como os meios que ela utiliza para cumprir sua finalidade.

Em particular, concentramos nossa atenção na falta de controle efetivo por parte da sociedade, explorando como a ANPD pode desempenhar um papel central na promoção da conscientização e no estabelecimento de um ambiente em que a privacidade individual e proteção dos dados sejam respeitadas e protegidas de maneira eficaz.

Ao longo deste estudo, destacamos a importância fundamental da ANPD na garantia dos direitos fundamentais de proteção de dados, privacidade e do cumprimento da Lei Geral de Proteção de Dados (Lei nº13.709/18).[3]

---

[3] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União,** Brasília, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 10 set. 2023.

2. Princípios de Proteção de Dados Pessoais

A evolução das leis de proteção de dados pessoais ao longo das décadas pode ser comparada a uma progressão geracional, um processo de adaptação às mudanças tecnológicas e às crescentes preocupações com a privacidade.[4] Essa metamorfose legal é, em si, uma expressão da busca constante por modelos jurídicos mais ricos e completos, capazes de acompanhar o ritmo frenético das inovações tecnológicas.

Essa transformação, embora tenha moldado a natureza das leis de proteção de dados, ainda pode ser sintetizada em princípios fundamentais que atravessam gerações e fronteiras jurídicas. Estes princípios, presentes em diferentes graus em várias jurisdições, refletem não apenas a convergência das soluções legislativas em todo o mundo, mas também a crescente ligação entre a proteção dos dados pessoais, a dignidade humana e os direitos fundamentais.[5]

Entre esses princípios, alguns têm raízes nas primeiras e segundas gerações de leis de proteção de dados e foram aprimorados pelas leis subsequentes. No entanto, muitos deles podem ser rastreados até discussões que surgiram na segunda metade da década de 1960, quando se debatia a criação do National Data Center nos Estados Unidos. Esse ambicioso projeto buscava estabelecer um banco de dados gigantesco para o uso da administração federal, embora tenha acabado por não se concretizar.[6]

---

[4] ANASTASIA, Vittoria Alvares; LARA, Caio Augusto Souza. O escândalo Cambridge Analytica: a manipulação de dados na era digital. **Percurso**, Curitiba, v.4. n. 31. p. 164-167, 2019. http://dx.doi.org/10.21902/ RevPercurso.2316-7521.v4i31.3722. Disponível em: http://revista.unicuritiba.edu.br/index.php/percurso/ article/download/3722/371372086. Acesso em: 10 set. 2023.

[5] BACHLECHNER, Daniel; FORS, Karolina La; SEARS, Alan M. The role of privacy-preserving technologies in the age of big data. In: PRE-ICIS WORKSHOP ON INFORMATION SECURITY AND PRIVACY, 13, 2018, São Francisco, USA. **Proceedings of the...** San Francisco: Association for Information Systems, 2018. Disponível em: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1009&context=wisp2018. Acesso em: 10 set. 2023.

[6] BARROS, Juliano Napoleão de. Big data, proteção de dados e transparência: desafios para a consolidação da confiança e garantia dos direitos do cidadão. **Revista Culturas Jurídicas**, v. 7, n. 17. P. 240-254, maio/ago. 2019. https://doi.org/10.22409/rcj.v7i17.868. Disponível em: https://periodicos.uff.br/culturasjuridicas/article/ view/45329/28902. Acesso em: 10 set. 2023.

O fracasso desse projeto centralizado não impediu que muitas das questões levantadas durante as discussões continuassem a ser exploradas, especialmente no contexto do tratamento de dados médicos por sistemas informatizados. No início da década de 1970, uma comissão de especialistas convocada pela Secretaria de Saúde, Educação e Bem-Estar dos EUA divulgou um estudo que destacava a ligação intrínseca entre a privacidade e o tratamento de dados pessoais, particularmente em relação às informações de saúde. Esse estudo ressaltou a necessidade de estabelecer regras claras para o controle das próprias informações pelos indivíduos.[7]

Essa conexão entre privacidade, controle sobre dados pessoais e proteção dos direitos fundamentais moldou a evolução das leis de proteção de dados pessoais em todo o mundo. À medida que a tecnologia avançava, esses princípios foram incorporados em leis mais modernas e abrangentes, refletindo uma preocupação crescente com a proteção da pessoa em um ambiente cada vez mais digitalizado.[8]

A jornada das leis de proteção de dados pessoais é uma história de adaptação, aprendizado e busca constante por uma maior proteção da privacidade e dos direitos fundamentais em um mundo impulsionado pela tecnologia. À medida que exploramos essas leis e suas origens, fica evidente que a proteção dos dados pessoais não é apenas uma questão de conformidade legal, mas uma expressão fundamental da dignidade humana e da autodeterminação informativa.[9]

A privacidade pessoal de um indivíduo é afetada diretamente pelo tipo de divulgação e utilização que é feita das informações registradas a seu respeito. Um tal registro, contendo informações sobre um indivíduo identificável deve, portanto, ser administrado com procedimentos que permitam a este indivíduo ter o direito de participar na sua decisão sobre qual deve ser o conteúdo deste registro e qual a divulgação e utilização a ser feita das informações pessoais nele contidas. Qualquer registro, divulgação e utilização das informações pessoais fora destes procedimentos não devem ser permitidas, por consistirem em uma prática desleal, a não ser que tal registro, utilização ou divulgação sejam autorizados por lei.

---

[7] BACHLECHNER; FORS; SEARS, *op. cit.*
[8] BARROS, *op. cit.*
[9] BAUMAN, Zygmunt. **Vigilância líquida.** Rio de Janeiro: Zahar, 2014.

Uma concepção como esta requer que sejam estabelecidos meios de garantia para o cidadão, que efetivamente vieram descritos como:

a) Não deve existir um sistema de armazenamento de informações pessoais cuja existência seja mantida em segredo.

b) Deve existir um meio para um indivíduo descobrir quais informações a seu respeito estão contidas em um registro e de qual forma ela é utilizada;

c) Deve existir um meio para um indivíduo evitar que a informação a seu respeito colhida para um determinado fim seja utilizada ou disponibilizada para outros propósitos sem o seu conhecimento;

d) Deve existir um meio para um indivíduo corrigir ou retificar um registro de informações a seu respeito.

e) Toda organização que estruture, mantenha, utilize ou divulgue registros com dados pessoais deve garantir a confiabilidade destes dados para os fins pretendidos e deve tomar as devidas precauções para evitar o mau uso destes dados.

Os princípios fundamentais que orientam a proteção de dados pessoais representam a espinha dorsal das legislações e tratados voltados para a preservação da privacidade em um mundo cada vez mais digital. Esses princípios, conhecidos como *Fair Information Principles*, estabelecem diretrizes essenciais que devem ser aplicadas na gestão e tratamento dos dados pessoais.[10]

A primeira dessas diretrizes é o Princípio da Publicidade, que preconiza que a existência de bancos de dados contendo informações pessoais deve ser de conhecimento público.[11] Isso pode ser alcançado por meio de autorizações prévias para sua criação, notificação às autoridades competentes sobre sua existência ou a

---

[10] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020.

[11] DETERMANN, Lothar. Determann's field guide to data privacy law – international corporate compliance. 2. ed. Massachusetts: Edward Elgar, 2015 *apud* SARLET, Gabrielle Bezerra Sales; RUARO, Regina Linden. A proteção de dados sensíveis no sistema normativo brasileiro sob o enfoque da Lei Geral de Proteção de Dados (LGPD) – L. 13.709/2018. **Revista Direitos Fundamentais & Democracia**, v. 26, n. 2, p. 81-106, 2021. https://doi.org/10.25192/issn.1982-0496.rdfd.v26i22172. Disponível em: https://revistaeletronicardfd.uni brasil.com.br/index.php/rdfd/article/view/2172/694. Acesso em: 10 set. 2023.

obrigação de enviar relatórios periódicos. A transparência é fundamental para garantir que os indivíduos saibam como seus dados estão sendo utilizados.[12]

Outro princípio crucial é o da Exatidão, que exige que os dados armazenados sejam precisos e reflitam a realidade. Isso implica a coleta e o tratamento cuidadoso das informações, bem como atualizações periódicas conforme necessário.[13] A integridade dos dados é essencial para garantir que as informações pessoais sejam usadas de maneira confiável.[14]

O Princípio da Finalidade estipula que qualquer uso de dados pessoais deve estar alinhado com a finalidade comunicada ao titular dos dados antes da coleta. Isso limita a transferência de dados para terceiros e estabelece critérios para avaliar a adequação do uso de dados para uma determinada finalidade. Esse princípio é fundamental para evitar abusos na utilização de informações pessoais.[15]

O Princípio do Livre Acesso garante que os indivíduos tenham o direito de acessar os bancos de dados que contêm suas informações pessoais. Isso permite que eles obtenham cópias de seus registros e exerçam controle sobre seus dados. Além disso, o acesso permite a correção de informações incorretas e a remoção de dados obsoletos ou irrelevantes.[16]

O Princípio da Segurança Física e Lógica estabelece a obrigação de proteger os dados contra riscos como extravio, destruição, modificação, transmissão não autorizada e acesso indevido. A segurança dos dados é essencial para evitar violações de privacidade e garantir a integridade das informações pessoais[17]

Esses princípios, embora possam ser adaptados e incorporados de diferentes maneiras nas leis de proteção de dados pessoais em todo o mundo, formam a base para abordar questões críticas relacionadas à privacidade.[18] Além disso, refletem a

[12] BONAVIDES, Paulo. **Teoria constitucional da democracia participativa**: por um direito constitucional de luta e resistência, por uma nova hermenêutica, por uma repolitização da legitimidade. São Paulo: Malheiros, 2001.
[13] DETERMANN, *op. cit.*
[14] BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil.** Brasília: Senado Federal, 1988.
[15] CASTELLS, Manuel. **A galáxia da internet**: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Zahar, 2003.
[16] CASTELLS, *op. cit.*
[17] CAVOUKIAN, Ann. Information & privacy: 7 foundational principles. Internet architecture board. 2011. Disponível em: https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf. Acesso em: 09 set. 2023.
[18] DETERMANN, *op. cit.*

tendência crescente de reconhecer a proteção de dados como um direito fundamental em várias jurisdições, incluindo em níveis constitucionais. Países como Espanha e Portugal, por exemplo, têm dispositivos em suas constituições que abordam a proteção da privacidade em um contexto cada vez mais informático.[19]

Por fim, esses princípios não apenas guiam as leis e regulamentações de proteção de dados pessoais, mas também representam um compromisso com a preservação da privacidade e a garantia de que os direitos fundamentais dos indivíduos sejam respeitados em uma era de constante avanço tecnológico.[20]

3. Desenvolvimento das Leis de Proteção de Dados

O tratamento autônomo da proteção de dados pessoais é uma tendência que hoje está firmemente enraizada em diversos ordenamentos jurídicos. Isso representa uma mudança notável na forma como encaramos a privacidade e a proteção dos dados pessoais. O que inicialmente parecia ser uma resposta pontual a desafios tecnológicos específicos evoluiu para se tornar um direito fundamental à proteção de dados.[21]

Essa evolução pode ser ilustrada através da classificação evolutiva das leis de proteção de dados pessoais proposta por Viktor Mayer-Scönberger, que identifica quatro gerações distintas de leis nessa área. A primeira geração de leis refletia o estado da tecnologia da época, com foco na regulamentação de bancos de dados centralizados e no controle do uso de informações pessoais pelo Estado.[22]

No entanto, essas leis logo se tornaram obsoletas com a proliferação de centros de processamento de dados e a crescente complexidade do ambiente digital. A segunda geração de leis, exemplificada pela Lei Francesa de Proteção de Dados Pessoais de 1978, destacou a importância da privacidade como uma liberdade

---

[19] BIONI, *op. cit.*
[20] DETERMANN, *op. cit.*
[21] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, v. 12, n. 2, p. 91-108, 2011. Disponível em: https://periodicos.unoesc.edu.br/espacojuridico/article/view/1315/658. Acesso em: 10 set. 2023.
[22] DETERMANN, *op. cit.*

negativa que deveria ser exercida diretamente pelo cidadão. Essas leis permitiram aos indivíduos identificar e contestar o uso indevido de seus dados pessoais.[23]

À medida que o fornecimento de dados pessoais se tornou essencial para a participação na vida social, uma terceira geração de leis surgiu na década de 1980. Essas leis reconheceram a complexidade do processo de proteção de dados, que vai além da simples autorização para a coleta e uso de informações pessoais. Elas abordaram a autodeterminação informativa, garantindo que os indivíduos pudessem tomar decisões informadas sobre seus dados em um contexto mais amplo.[24]

A autodeterminação informativa tornou-se uma extensão das liberdades protegidas pelas leis de segunda geração, incluindo o direito de participar ativamente do processo de tratamento de dados e o direito à informação. Essas mudanças refletem uma compreensão mais sofisticada da proteção de dados como um processo complexo que envolve a participação ativa dos indivíduos na sociedade.[25]

O tratamento autônomo da proteção de dados pessoais representa uma mudança profunda na forma como concebemos a proteção da privacidade. Evoluímos de um modelo centrado no controle estatal e na autorização para um modelo que coloca o cidadão no centro do processo, permitindo-lhe tomar decisões informadas sobre seus próprios dados pessoais. Esse desenvolvimento é um reflexo da importância crescente da proteção de dados na era digital e da necessidade de garantir que os direitos individuais sejam respeitados em um mundo cada vez mais orientado pela tecnologia.[26]

Nessa evolução, é importante destacar a Lei de Acesso à Informação (Lei nº 12.527/2011)[27] e o assim chamado Marco Civil da Internet (Lei nº 12.965/2014) e o

---

[23] DETERMANN, *op. cit.*

[24] GEDIEL, José Antônio Peres; CORRÊA, Adriana Espíndola. Proteção jurídica de dados pessoais: a intimidade sitiada entre o estado e o mercado. **Revista da Faculdade de Direito UFPR**, Curitiba, n. 47, p. 141-147, 2008. http://dx.doi.org/10.5380/rfdufpr.v47i0.15738. Disponível em: https://revistas.ufpr.br/direito/article/download/ 15738/10444. Acesso em: 10 set. 2023.

[25] DETERMANN, *op. cit.*

[26] GARCIA, 2023, *op. cit.*

[27] BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. **Diário Oficial da União**, Brasília, 18 nov. 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 09 set. 2023.

respectivo Decreto que o regulamentou (Decreto nº 8.771/2016), mas especialmente a Lei Geral de Proteção de Dados, LGPD (Lei nº 13.709, de 2018).

A LGPD tem como principal objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Também tem como foco a criação de um cenário de segurança jurídica, com a padronização de regulamentos e práticas para promover a proteção aos dados pessoais de todo cidadão que esteja no Brasil, de acordo com os parâmetros internacionais existentes.

No Brasil, podemos definir a Lei Geral de Proteção de Dados (LGPD) como uma legislação que trata da proteção e garantias dos titulares de dados. Com a EC nº 115/2022[28], foi acrescido o direito à proteção dos dados pessoais como um direito fundamental, inclusive nos meios digitais" (Incluído pela Emenda Constitucional nº 115, de 2022).

O direito fundamental à proteção de dados assume grande relevância, pelo fato da existência de uma série de lacunas regulatórias, posto que a LGPD possui restrições em sua aplicação.

4. A Proteção de Dados: Salvaguardando a Privacidade na Era Digital

A proteção de dados tornou-se um tópico de extrema importância na sociedade contemporânea, à medida que vivemos cada vez mais em um mundo digitalizado e interconectado. Com a crescente quantidade de informações pessoais e sensíveis sendo coletadas, armazenadas e processadas por empresas e governos, a necessidade de salvaguardar a privacidade dos indivíduos nunca foi tão premente.[29]

---

[28] BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. **Diário Oficial da União**, Brasília, 11 fev. 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#art1. Acesso em: 09 set. 2023.

[29] MAGRANI, Eduardo; OLIVEIRA, Renan Medeiros de. A internet das coisas e a lei geral de proteção de dados: reflexões sobre os desafios do consentimento e do direito à explicação. **Revista do Advogado**, São Paulo, n. 144, p. 80-89, nov. 2019.

A proteção de dados refere-se ao conjunto de práticas e regulamentos destinados a garantir que as informações pessoais de um indivíduo sejam tratadas com responsabilidade, transparência e segurança. Isso envolve não apenas os dados pessoais, como nomes, endereços e números de identificação, mas também dados sensíveis, como informações médicas, financeiras e genéticas.[30]

Um dos marcos mais significativos na proteção de dados foi a introdução do Regulamento Geral de Proteção de Dados (RGPD) na União Europeia em 2018. O RGPD estabeleceu um conjunto abrangente de regras para a coleta e processamento de dados pessoais, garantindo que as empresas e organizações que operam na UE respeitem a privacidade de seus cidadãos. Além disso, forneceu diretrizes claras sobre a obtenção de consentimento, notificação de violações de dados e o direito das pessoas de acessar e controlar seus próprios dados.[31]

No entanto, a proteção de dados não é apenas uma preocupação europeia. Em todo o mundo, governos estão implementando regulamentos semelhantes, como a Lei de Proteção de Dados Pessoais no Brasil e o *California Consumer Privacy Act* (CCPA) nos Estados Unidos. Essas leis visam criar um ambiente onde a privacidade seja valorizada e respeitada, independentemente de onde você esteja geograficamente.[32]

As empresas também têm um papel crucial a desempenhar na proteção de dados. Elas devem adotar práticas de coleta e armazenamento de dados que sejam éticas e seguras. Isso inclui investir em tecnologias de segurança cibernética, treinar seus funcionários sobre boas práticas de proteção de dados e nomear um encarregado de proteção de dados (DPO) responsável por garantir a conformidade com as leis de privacidade.[33]

Além disso, os indivíduos também desempenham um papel vital na proteção de seus próprios dados. Eles devem estar cientes de seus direitos de privacidade,

---

[30] MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coord.). **LGPD: Lei Geral de Proteção de Dados comentada**. 2. ed. São Paulo: Thomson Reuters, 2020.

[31] MASILI, Clarissa Menezes Vaz. **Regulação do uso de dados pessoais no Brasil**: papel do usuário na defesa de um direito à tutela de dados pessoais autônomo. 2018. Dissertação (Mestrado) – Faculdade de Direito da Universidade de Brasília, Brasília, 2016. Disponível em: http://icts.unb.br/jspui/bitstream/10482/34290/3/ 2018_ClarissaMenezesVazMasili.pdf. Acesso em: 10 set. 2023.

[32] MASILI, *op. cit.*

[33] MASILI, *op. cit.*

tomar medidas para proteger suas informações pessoais, como o uso de senhas fortes e a autenticação de dois fatores, e ser seletivos ao compartilhar informações com terceiros.[34]

Em última análise, a proteção de dados é uma questão de equilíbrio entre a necessidade legítima de coletar e usar dados para fins comerciais e governamentais e o direito fundamental à privacidade.[35] É um desafio contínuo na era digital em constante evolução, que exige um compromisso constante com a ética e a segurança por parte de todos os envolvidos. À medida que avançamos na era da informação, a proteção de dados continuará sendo um tema crucial que molda nossa sociedade e nossa relação com a tecnologia.[36]

5. A Autoridade Nacional de Proteção de Dados, Papéis e Responsabilidades

A Autoridade Nacional de Proteção de Dados (ANPD) é uma autarquia de natureza especial, vinculada ao Ministério da Justiça e Segurança Pública, responsável por zelar pela proteção de dados pessoais e por regulamentar, implementar e fiscalizar o cumprimento da LGPD no Brasil.

Criada em razão da Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº13.709, de 2018), a ANPD tem a atribuição de fiscalizar e zelar pela proteção dos dados pessoais, assegurar a observância de segredos comerciais e industriais e punir eventuais descumprimentos à legislação e ainda, possui um papel "educador" e fomentador da cultura de proteção de dados das empresas, órgãos, entidades e da sociedade como um todo, de fiscalização e aplicação de sanções em casos de tratamento de dados em desacordo com a legislação, garantindo o devido processo administrativo e o direito de recurso.

A LGPD estabelece um papel significativo para a ANPD, devendo esta, garantir que dados pessoais sejam protegidos de acordo com as regras da LGPD (Artigo 55-J-I) através da emissão de opiniões técnicas e diretrizes (Artigo 55-J-XX), educação (Artigo 55-J-VI), execução de sanções por descumprimento (Artigo 55-JIV),

---

[34] MAGRANI; OLIVEIRA, *op. cit.*
[35] MAGRANI; OLIVEIRA, *op. cit.*
[36] MASILI, *op. cit.*

recebimento e tratamento de reclamações e perguntas (Artigo 55-J-V), cooperação internacional (Artigo 55-J-IX) e edição de regulamentos e procedimentos sobre proteção de dados pessoais e privacidade (Artigo 55-J-XIII).

O art. 55-J da LGPD estabelece as principais competências da ANPD, dentre as quais se destacam as seguintes:

> a) Elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;
> b) Fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;
> c) Promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança;
> d) Estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis;
> e) Promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional;
> f) Editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD;
> g) Ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento;
> h) Editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se à Lei;
> i) Deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação da LGPD, as suas competências e os casos omissos;

j) Articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e

k) Implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com a LGPD.

As responsabilidades da ANPD coadunam em proteger os indivíduos e seus direitos fundamentais, garantindo que o desenvolvimento econômico, digital e social do Brasil esteja alinhado com os princípios de privacidade e proteção aos dados pessoais, de modo a assegurar à efetividade da LGPD e demais legislações atinentes ao tema.

6. A Proteção de Dados como um Direito Fundamental e a Necessidade de Fiscalização da Autoridade Nacional de Proteção de Dados

Em uma era em que nossas vidas são cada vez mais entrelaçadas com a tecnologia e nossas informações pessoais circulam pela vasta rede digital, a proteção de dados emergiu como um direito fundamental inquestionável. Esse direito não se limita apenas à garantia de que nossas informações pessoais sejam tratadas com respeito e segurança, mas também representa um pilar essencial para a manutenção da dignidade, liberdade e privacidade dos cidadãos.[37]

Em muitos países, a conscientização sobre a importância da proteção de dados se traduziu em legislações robustas e abrangentes. Um exemplo notável é o Regulamento Geral de Proteção de Dados (RGPD) na União Europeia, que fornece um modelo sólido para a proteção de dados pessoais. No entanto, criar leis por si só não é suficiente; é necessário um órgão regulador competente para garantir a efetivação desses direitos.[38]

---

[37] MASSON, Nathalia. **Manual de direito constitucional**. 8. ed. Salvador: Juspodivm, 2020.

[38] MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional**. 16. ed. São Paulo: Saraiva Educação, 2021.

Foi aprovada PEC 17/2020 com posterior promulgação da EC 115/22, em fevereiro de 2022 e a discussão sobre a conveniência e inserção de um direito à proteção de dados pessoais na Constituição Federal de 1988 (CF), ficou superada. De acordo com o texto da EC 115, foi acrescido o inciso LXXIX ao artigo 5º, CF, dispondo que "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais".

Os direitos fundamentais possuem *status* normativo superior em relação a todo o restante do ordenamento jurídico nacional. Assim, na condição de direito fundamental, assume a condição de limite material à reforma constitucional, devendo, ademais disso, serem observados os assim chamados limites formais, circunstanciais e temporais, nos termos do artigo 60, parágrafos 1 a 4º, da CF.

As normas relativas ao direito à proteção de dados são dotadas de aplicabilidade imediata (direta) e vinculam diretamente todos os atores públicos, bem como sopesadas as devidas ressalvas os atores privados (Artigo 5º, º 1º, CF).

A Autoridade Nacional de Proteção de Dados (ANPD) é a entidade responsável por supervisionar a aplicação das leis de proteção de dados, garantindo que as organizações e os governos cumpram suas obrigações legais em relação à privacidade dos indivíduos. Essa autoridade não apenas fiscaliza, mas também educa, orienta e colabora com diferentes partes interessadas para promover uma cultura de proteção de dados.[39]

A necessidade de uma autoridade de proteção de dados é clara por várias razões, vejamos:

> a) Sem uma supervisão eficaz, as organizações podem negligenciar suas obrigações de proteção de dados. A ANPD age como um árbitro imparcial, garantindo que todos cumpram as mesmas regras.[40]
>
> b) Quando ocorre uma violação de dados, a ANPD pode conduzir investigações, impor sanções e garantir que as vítimas sejam devidamente notificadas. Isso cria

---

[39] MORAES, Alexandre de. **Direitos humanos fundamentais**: teoria geral. 12 ed. São Paulo: Atlas, 2021.

[40] NOGUEIRA, Fernanda Araújo Couto e Melo; FONSECA, Maurício Leopoldino da. O consentimento na lei geral de proteção de dados: autonomia privada e o consentimento livre, informado, específico e expresso. In: GROSSI, Bernardo Menicucci (Org.). **Lei geral de proteção de dados**: uma análise preliminar da Lei 13.709/2018 e da experiência de sua implantação no contexto empresarial. Porto Alegre: Editora Di, 2020. p. 15-44.

responsabilidade e incentiva as organizações a investirem em medidas de segurança adequadas.[41]

c) A ANPD não apenas pune, mas também fornece orientações e recursos para ajudar as organizações a compreender e cumprir as leis de proteção de dados. Isso é especialmente útil para pequenas empresas que podem não ter recursos para especialistas em privacidade.[42] Ela age como um guardião dos direitos dos cidadãos, permitindo que saibam que há uma entidade a quem recorrer caso suspeitem de abuso de dados pessoais.[43]

A proteção de dados é, sem dúvida, um direito fundamental que merece nossa atenção e respeito. No entanto, para que esse direito seja verdadeiramente eficaz, a presença de uma Autoridade Nacional de Proteção de Dados é essencial. Ela desempenha um papel fundamental na fiscalização, regulamentação e promoção de uma cultura de respeito à privacidade em um mundo digital em constante evolução.

É através da colaboração entre governos, organizações e indivíduos, com o apoio de entidades como a ANPD, que podemos alcançar uma proteção de dados efetiva e garantir que nossos direitos fundamentais sejam preservados na era digital.[44]

Educar os indivíduos e as organizações a respeito da proteção de dados pessoais é fundamental para a eficácia das garantias. Os titulares de dados devem ter um entendimento, ainda que básico, de como podem controlar seus dados pessoais, e, devem ainda, ser capazes de confiar no tratamento que assegura a proteção de dados.

Nesta seara, as organizações devem ser conscientizadas de suas obrigações e responsabilidades para com os titulares de dados, adotando medidas protetivas adequadas e assumir as responsabilidades para poder gerar confiabilidade no tratamento de dados apto a garantir o direito fundamental. A ANPD tem um papel

---

[41] PEREZ LUÑO, Antonio-Enrique. Teledemocracia, ciberciudadania y derechos humanos. **Revista Brasileira de Políticas Públicas,** Brasília, v. 4. n. 2. p. 9-45, 2014. http://doi.org/10.5102/rbpp.v4i2.2835. Disponível em: https://www.publicacoesacademicas.uniceub.br/RBPP/article/download/2835/pdf. Acesso em: 10 set. 2023.

[42] PINHEIRO, Patrícia Pack. Direito digital. 7. ed. São Paulo: Saraiva, 2021.

[43] NOGUEIRA; FONSECA, *op. cit.*

[44] PEREZ LUÑO, *op. cit.*

crucial na educação das pessoas envolvidas na esfera do tratamento de dados, devendo atuar de forma colaborativa e construtiva com eles.

Neste contexto, podemos indicar que a ANPD, através de seu site[45] e demais meios, busca fomentar o tema e cumprir suas atribuições com diversas medidas, tais como; orientações, regulamentos, documentos, diretrizes de procedimentos, e, disponibilizando ainda, agendas institucionais e audiências públicas.

Assim, podemos definir a necessidade de uma atuação forte e eficaz da ANPD para que seja possível alcançar os objetivos de regulamentar, implementar e fiscalizar o cumprimento da LGPD e demais legislações, bem como garantir a observância aos direitos fundamentais de privacidade e proteção de dados.

Conclusão

Em conclusão, a evolução das leis de proteção de dados ao longo do tempo representa uma resposta contínua e adaptativa às transformações tecnológicas e às crescentes preocupações com a privacidade. Os princípios fundamentais que subjazem a essas leis, como transparência, precisão, propósito, acesso e segurança, servem como alicerce para a proteção global dos dados pessoais.

A transição em direção a um tratamento autônomo dos dados pessoais, dando aos indivíduos o controle sobre suas informações, marca uma mudança significativa na abordagem à privacidade e à proteção de dados. Isso coloca o cidadão no epicentro do processo e reflete a crescente relevância da proteção de dados em nossa era digital.

Além disso, a proteção de dados se tornou um pilar essencial em nosso mundo digital, com regulamentos rigorosos como o RGPD estabelecendo normas elevadas. As empresas desempenham um papel vital ao adotar práticas éticas e seguras, enquanto os indivíduos também compartilham responsabilidades na proteção de suas informações pessoais.

No Brasil, embora tenhamos o histórico de outras legislações aplicáveis ao tema, a Lei Geral de Proteção de Dados (LGPD) é uma legislação que trata da

---

[45] BRASIL. Ministério da Justiça e Segurança Pública. **Autoridade Nacional de Proteção de Dados**. Brasília: MJSP, 2023. Disponível em: https://www.gov.br/anpd/pt-br. Acesso em: 12 set. 2023.

proteção e garantias dos titulares de dados. Com a EC 115/2022, foi acrescido o inciso LXXIX ao artigo 5º, CF, dispondo que assegura, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais. Assim, o direito fundamental à proteção de dados assumiu grande relevância, pelo fato da existência de uma série de lacunas regulatórias e face às restrições de aplicação da LGPD.

Podemos afirmar que, a presença de autoridades de proteção de dados, exemplificada pela Autoridade Nacional de Proteção de Dados (ANPD) é imperativa para assegurar que as leis sejam cumpridas e para fomentar uma cultura de proteção de dados. Resta clara, portanto, a necessidade de uma atuação forte e eficaz para que seja possível alcançar os objetivos de regulamentar, implementar e fiscalizar o cumprimento da LGPD e demais legislações, bem como garantir a observância aos direitos fundamentais de privacidade e proteção de dados.

Foi possível concluir que a ANPD, dentre suas atribuições, possui um papel fundamental em educar e orientar os indivíduos e as organizações a respeito da proteção de dados pessoais em busca de efetivar as garantias legais. Isso porque, os indivíduos titulares de dados devem ter um entendimento de como podem controlar seus dados pessoais e devem ser capazes de confiar no tratamento que assegura a proteção de dados, bem como as organizações devem ser conscientizadas de suas obrigações e responsabilidades para com os titulares de dados, adotando medidas protetivas adequadas a assumir as responsabilidades e gerar a confiabilidade no tratamento de dados apto a garantir de modo eficaz, dentre outros, o direito fundamental da proteção dos dados.

Em última análise, observou-se que a proteção de dados não é apenas um direito fundamental, mas também uma responsabilidade coletiva. Sua preservação, em especial na era digital, requer uma colaboração estreita entre governos, organizações e indivíduos, com o apoio essencial da ANPD, devendo esta, adotar medidas e meios para fomentar e direcionar os envolvidos ao tema, cumprindo seus papéis e responsabilidades de forma assertiva.

Referências

ANASTASIA, Vittoria Alvares; LARA, Caio Augusto Souza. O escândalo *Cambridge Analytica*: a manipulação de dados na era digital. **Percurso**, Curitiba, v.4. n. 31. p. 164-167, 2019. http://dx.doi.org/10.21902/RevPercurso.2316-7521.v4i31.3722. Disponível em: http:// revista.unicuritiba.edu.br/index.php/percurso/article/download/3722/371372086. Acesso em: 10 set. 2023.

BACHLECHNER, Daniel; FORS, Karolina La; SEARS, Alan M. The role of privacy-preserving technologies in the age of big data. In: PRE-ICIS WORKSHOP ON INFORMATION SECURITY AND PRIVACY, 13, 2018, São Francisco, USA. **Proceedings of the…** San Francisco: Association for Information Systems, 2018. Disponível em: https:// aisel.aisnet.org/cgi/viewcontent.cgi?article=1009&context=wisp2018. Acesso em: 10 set. 2023.

BARROS, Juliano Napoleão de. Big data, proteção de dados e transparência: desafios para a consolidação da confiança e garantia dos direitos do cidadão. **Revista Culturas Jurídicas,** v. 7, n. 17. P. 240-254, maio/ago. 2019. https://doi.org/10.22409/rcj.v7i17.868. Disponível em: https://periodicos.uff.br/culturasjuridicas/article/view/45329/28902. Acesso em: 10 set. 2023.

BAUMAN, Zygmunt. **Vigilância líquida**. Rio de Janeiro: Zahar, 2014.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020.

BONAVIDES, Paulo. **Teoria constitucional da democracia participativa**: por um direito constitucional de luta e resistência, por uma nova hermenêutica, por uma repolitização da legitimidade. São Paulo: Malheiros, 2001.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil.** Brasília: Senado Federal, 1988.

BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. **Diário Oficial da União**, Brasília, 11 fev. 2022. Disponível em: http://www. planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#art1. Acesso em: 09 set. 2023.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990;

revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. **Diário Oficial da União**, Brasília, 18 nov. 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 09 set. 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**, Brasília, 15 ago. 2018. Disponível em: http://www. planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 10 set. 2023.

BRASIL. Ministério da Justiça e Segurança Pública. **Autoridade Nacional de Proteção de Dados.** Brasília: MJSP, 2023. Disponível em: https://www.gov.br/anpd/pt-br. Acesso em: 12 set. 2023.

BRASIL. Ministério da Justiça e Segurança Pública. **Proteção de dados pessoais agora é um direito fundamental**. Brasília: MJSP, 2022. Disponível em: https://www.gov.br/anpd/pt-br/protecao-de-dados-pessoais-agora-e-um-direito-fundamental. Acesso em: 12 set. 2023.

CASTELLS, Manuel. **A galáxia da internet**: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Zahar, 2003.

CAVOUKIAN, Ann. Information & privacy: 7 foundational principles. Internet architecture board. 2011. Disponível em: https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf Acesso em: 09 set. 2023.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, v. 12, n. 2, p. 91-108, 2011. Disponível em: https://periodicos.unoesc.edu.br/ espacojuridico/article/view/1315/658. Acesso em: 10 set. 2023.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters, 2020.

GEDIEL, José Antônio Peres; CORRÊA, Adriana Espíndola. Proteção jurídica de dados pessoais: a intimidade sitiada entre o estado e o mercado. **Revista da Faculdade de Direito UFPR**, Curitiba, n. 47, p. 141-147, 2008. http://dx.doi.org/10.5380/rfdufpr.v47i0.15738. Disponível em: https://revistas.ufpr.br/direito/article/download/15738/10444. Acesso em: 10 set. 2023.

MAGRANI, Eduardo; OLIVEIRA, Renan Medeiros de. A internet das coisas e a lei geral de proteção de dados: reflexões sobre os desafios do consentimento e do direito à explicação. **Revista do Advogado**, São Paulo, n. 144, p. 80-89, nov. 2019.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coord.). **LGPD: Lei Geral de Proteção de Dados comentada**. 2. ed. São Paulo: Thomson Reuters, 2020.

MASILI, Clarissa Menezes Vaz. **Regulação do uso de dados pessoais no Brasil**: papel do usuário na defesa de um direito à tutela de dados pessoais autônomo. 2018. Dissertação (Mestrado) – Faculdade de Direito da Universidade de Brasília, Brasília, 2016. Disponível em: http://icts.unb.br/jspui/bitstream/10482/34290/3/2018_ClarissaMenezesVazMasili.pdf. Acesso em: 10 set. 2023.

MASSON, Nathalia. **Manual de direito constitucional**. 8. ed. Salvador: Juspodivm, 2020.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional.** 16. ed. São Paulo: Saraiva Educação, 2021.

MORAES, Alexandre de. **Direitos humanos fundamentais**: teoria geral. 12 ed. São Paulo: Atlas, 2021.

MOURA, Clarissa Maria Lima. **Dados pessoais como ativo na economia digital**: a tutela jurídica na legislação nacional e europeia acerca da manipulação de dados sensíveis para fins econômicos. 2019. Monografia (Conclusão de Curso de Direito) - Faculdade de Direito da Universidade Federal de Pernambuco, Recife, 2019. Disponível em: https://repositorio.ufpe. br/handle/123456789/37157. Acesso em: 10 set. 2023.

NOGUEIRA, Fernanda Araújo Couto e Melo; FONSECA, Maurício Leopoldino da. O consentimento na lei geral de proteção de dados: autonomia privada e o consentimento livre, informado, específico e expresso. In: GROSSI, Bernardo Menicucci (Org.). **Lei geral de proteção de dado**s: uma análise preliminar da Lei 13.709/2018 e da experiência de sua implantação no contexto empresarial. Porto Alegre: Editora Di, 2020. p. 15-44.

PEREZ LUÑO, Antonio-Enrique. Teledemocracia, ciberciudadania y derechos humanos. **Revista Brasileira de Políticas Públicas,** Brasília, v. 4. n. 2. p. 9-45, 2014. http://doi.org/ 10.5102/rbpp.v4i2.2835. Disponível em: https://www.publicacoesacademicas.uniceub.br/RBPP/article/download/2835/pdf. Acesso em: 10 set. 2023.

PINHEIRO, Patrícia Pack. **Direito digital**. 7. ed. São Paulo: Saraiva, 2021.

SARLET, Gabrielle Bezerra Sales; RUARO, Regina Linden. A proteção de dados sensíveis no sistema normativo brasileiro sob o enfoque da Lei Geral de Proteção de Dados (LGPD) – L. 13.709/2018. **Revista Direitos Fundamentais & Democracia**, v. 26, n. 2, p. 81-106, 2021. https://doi.org/10.25192/issn.1982-0496.rdfd.v26i22172. Disponível em: https://revista

eletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/2172/694. Acesso em: 10 set. 2023.

SARLET, Ingo Wolfgang. A EC 115/22 e a proteção de dados pessoais como direito fundamental. **Consultor Jurídico**, 11 mar. 2022. Disponível em: https://www.conjur.com.br/2022-mar-11/direitos-fundamentais-ec-11522-protecao-dados-pessoais-direito-fundamental. Acesso em: 10 set. 2023.

9. A PROTEÇÃO MULTINÍVEL DOS DADOS PESSOAIS COMO DIREITO INTERNACIONAL HUMANO

https://doi.org/10.36592/9786554600798-09

Stella Muniz Campos Elias[1]

RESUMO

A Lei Geral de Proteção de Dados – LGPD trouxe ao ordenamento jurídico brasileiro a proteção dos dados pessoais, para que os indivíduos possam gerenciar os tratamentos dos próprios dados dentro das empresas, sejam estas públicas ou privadas. Neste sentido, ao se falar em dados pessoais, fala-se em vida privada dos seres humanos e, portanto, trata-se de um direito protegido tanto em um plano infraconstitucional, com a LGPD, quanto constitucional, quando tratamos dos direitos fundamentais do artigo 5º da CF. E, indo além, ao relacionar a vida privada à utilização de dados pessoais, tem-se uma proteção dentro do sistema internacional dos direitos humanos, precisamente no artigo 12 da Declaração Universal dos Direitos Humanos, cuja garantia não só abrange a proteção das pessoas humanas quanto à privacidade, mas também quanto aos dados pessoais, o que resulta em uma verdadeira proteção multinível destes direitos.
Palavras-chave: Lei Geral de Proteção de Dados; Direito Fundamental; Vida Privada; Sistema Internacional dos Direitos Humanos; Proteção Multinível dos Dados Pessoais.

1. INTRODUÇÃO

A Lei nº 13.709 de 14 de agosto de 2018, mais conhecida como a Lei Geral de Proteção de Dados – LGPD, trouxe uma proteção específica aos dados pessoais dos indivíduos ao serem tratados ou armazenados dentro das corporações, sejam elas públicas ou privadas, alcançando desde as empresas sem fins lucrativos, as individuais, as pequenas, médias e grandes empresas até as multinacionais.

---

[1] Advogada Empresarial. Mestra pelo Programa de Pós-Graduação *stricto sensu* em Direito da Pontifícia Universidade Católica de Minas Gerais – PUC Minas. Pós-Graduada em Direito do Trabalho e Processo do Trabalho pela Pontifícia Universidade Católica de Minas Gerais – PUC Minas. Pós-graduada em Docência com Ênfase Jurídica. Consultora e Especialista em Proteção de Dados. Consultora e Especialista em Proteção Trabalhista. Membro consultora da Comissão Especial de Proteção de Dados da OAB Nacional. Vice-presidente da Comissão de Proteção de Dados da OAB/MG. Membro do Programa e da Comissão do Direito na Escola. Membro da Comissão de Direitos Sociais e Trabalhistas da OAB/MG. Membro do Grupo de Pesquisa e Extensão Capitalismo e Proteção Social na Perspectiva dos Direitos Humanos e Fundamentais do Trabalho e da Seguridade Social. E-mail: contato@stellacampos.com.br

Ao proteger os dados pessoais da pessoa física, esta lei nos remete, inicialmente, aos aspectos da personalidade civil da pessoa natural, cuja previsão está na Parte Geral do Código Civil e a qual estabelece a proteção dos bens inerentes à pessoa humana, tais como o nome e a vida privada.

Neste sentido, também há no nosso ordenamento jurídico a Lei nº 12.965 de 2014, conhecida como Lei do Marco Civil da Internet, que regula direitos e deveres dos internautas na navegação, com o intuito de proteger os dados pessoais e a privacidade dos usuários.

Além disso, a Constituição da República de 1988 também prevê expressamente a proteção dos direitos fundamentais à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, assim como o "direito à proteção dos dados pessoais, inclusive nos meios digitais", no art. 5º, LXXIX.

Neste compasso, é necessário ir além e trazer para esta análise a proteção dos dados pessoais como expressão dos Direitos Humanos, uma vez que a própria Declaração Universal de Direitos Humanos já versava, em 1948, sobre a tutela à vida privada.

Com isso, verifica-se que a proteção de dados pessoais tem proteção não só infraconstitucional, mas também tem proteção constitucional e, indo além, tem ampla tutela internacional.

Essa proteção multinível dos dados pessoais faz com que o indivíduo tenha um verdadeiro direito humano à proteção da privacidade, intimidade, vida privada e aos dados pessoais e, consequentemente, estes direitos são inerentes à pessoa humana detentora da titularidade destes dados pessoais, não conseguindo se desvencilhar de tais direitos.

Dessa forma, o presente artigo demonstrará que a legislação existente não pode separar a proteção ao direito humano à intimidade, vida privada, privacidade e, especialmente, aos dados pessoais dentro da essência humana, sendo o estudo dividido em três capítulos e a conclusão. O primeiro tratará sobre a previsão legal dos direitos de personalidade no direito infraconstitucional e a proteção de dados no direito brasileiro. Já o segundo abordará sobre a proteção constitucional e as peculiaridades da privacidade no ordenamento jurídico pátrio e, por fim, o último capítulo versará sobre a proteção dos dados pessoais como direitos humanos.

2. A PREVISÃO LEGAL INFRACONSTITUCIONAL DOS DIREITOS DE PERSONALIDADE E A PROTEÇÃO DE DADOS NO DIREITO BRASILEIRO

Inicialmente, não podemos pensar na proteção dos dados pessoais sem antes discorrer sobre os direitos de personalidade, os quais são definidos, de acordo com Maria Helena Diniz[2] como sendo "os direitos subjetivos da pessoa de defender o que lhe é próprio, ou seja, a identidade, a liberdade, a sociabilidade, a reputação, a honra, a autoria etc.".

Esta abordagem se faz necessária, uma vez que a própria Lei Geral de Proteção de Dados – LGPD indica, dentre outros, o direito à privacidade como um de seus fundamentos legais, direito este que integra o direito de personalidade.

Portanto, imperioso apontar as normas legais que tratam sobre o direito à privacidade tanto no Código Civil de 2002 quanto na Lei do Marco Civil da Internet de 2014, antes mesmo de adentrar na proteção específica dos dados pessoais.

Vale ressaltar que, o direito à privacidade possui origem burguesa e, de maneira geral, permaneceu restrito à burguesia até o final da primeira metade do século XX. Este cenário começou a apresentar mudanças mais significativas no decorrer da década de 1960, tendo impulsionado, sobretudo, o aumento da circulação de informações, vez que houve ascensão do aprimoramento tecnológico na coleta de informações, o que resultou em uma "capacidade técnica cada vez maior de recolher, processar e utilizar a informação".[3]

Neste sentido, o art. 21 do Código Civil dispõe que "a vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma".

Dessa forma, verifica-se que a privacidade, por ser um dos direitos de personalidade trazidos pelo próprio Código Civil, não pode ser violada, salvo os casos

---

[2] DINIZ, Maria Helena. Curso de direito civil brasileiro. Teoria do direito civil. 29ª ed. São Paulo: Saraiva, 2012

[3] DONEDA, Danilo. Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade. Disponível em: <https://www.academia.edu/23345532/Considera%C3%A7%C3%B5es_iniciais_sobre_os_bancos_de_dados_informatizados_eo_direito_%C3%A0_privacidade>. Acesso em: 13.dez.2020.).

excepcionais expressamente previstos na lei, devendo o judiciário, inclusive, intervir quando motivado para garantir que esta norma seja devidamente cumprida.

Neste compasso, o art. 3º, inciso II, da Lei do Marco Civil da Internet, traz como princípio, dentre outros, a proteção da privacidade, além de estabelecer, no inciso III do mesmo artigo, a proteção expressa dos dados pessoais.

Além destes artigos, a Lei do Marco Civil da Internet também fixou explicitamente, no art. 7º, tanto os direitos e garantias do usuário quanto a proteção ao direito à privacidade, assim como garantiu expressamente, no art. 8º, que o direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.

Por fim, a Lei Geral de Proteção de Dados veio para dar ainda mais proteção ao tratamento dos dados pessoais dos indivíduos, visando garantir que o titular dos dados seja cientificado de todo e qualquer tratamento de seu dado pelas empresas, fixando, inclusive, diversas sanções administrativas diferentes para penalizar aquele que descumprir as regras estabelecidas e lesar os titulares dos dados.

Com isso, verifica-se que a proteção aos dados das pessoas, apesar de atualmente ter normas específicas, sempre esteve ligada ao direito à vida privada, direito este inserido no rol exemplificativo dos direitos de personalidade.

3. A PROTEÇÃO CONSTITUCIONAL DA PRIVACIDADE E SUAS PECULIARIEDADES NO ORDENAMENTO JURÍDICO PÁTRIO

A Constituição da República de 1988 estabeleceu no rol dos direitos fundamentais do art. 5º, mais especificadamente no inciso X, que os direitos à intimidade, à vida privada, à honra e à imagem das pessoas são invioláveis.

Em 2022, foi promulgada a EC 115, a qual incluiu o inciso LXXIX ao mesmo artigo anteriormente citado, que expressamente passou a garantir que a proteção aos dados pessoais fosse elevada para tratamento no plano dos direitos e garantias fundamentais.

Neste sentido, a EC 115/2022, também incluiu o inciso XXVI do art. 21, para estabelecer que compete à União "organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei", bem como fixou a competência privativa deste

ente federativo, no inciso XXX do art. 22, para legislar sobre a "proteção e tratamento de dados pessoais".

Dito isto, vale pontuar que privacidade ou vida privada, de acordo com Bernardo Gonçalves Fernandes (FERNANDES, Bernardo Gonçalves. Curso de Direito Constitucional. 7ª ed. Salvador: Juspodvm, 2015), é um "direito que um indivíduo tem de se destacar (se separar) de um grupo, isolando-se da observação do mesmo ou como, ainda, o direito ao controle das informações veiculadas sobre si mesmo."

Além disso, Fernandes[4] também pontua que:

> "a restrição ao direito à privacidade", somente pode ocorrer a partir do consentimento daquela própria pessoa, uma vez que "os direitos fundamentais, mesmo não sendo passíveis de renúncia plena, comportam formas de autolimitação. Se a restrição é feita espontaneamente, com o seu titular falando sobre sua intimidade como em uma entrevista, o caso é de mais fácil problematização."

Dessa forma, nota-se que já havia uma garantia constitucional aos direitos inerentes à pessoa humana, em especial quanto ao direito à privacidade, e que, com a importância do tema à sociedade civil, elevou a proteção aos dados pessoais das pessoas físicas ao *status* constitucional, sendo diretamente ligada à vida privada, vez que ambos pertencem ao indivíduo e são tutelados pelo direito de personalidade.

4. A PROTEÇÃO DOS DADOS PESSOAIS COMO EXPRESSÃO DOS DIREITOS HUMANOS

No Brasil, a proteção inequívoca à vida privada das pessoas se fundamenta juridicamente tanto no Código Civil quanto na Lei do Marco Civil da Internet, além de também ser expressamente tutelada na Constituição da República.

Mas devemos ir além das fronteiras do ordenamento jurídico pátrio.

---

[4] FERNANDES, Bernardo Gonçalves. Curso de Direito Constitucional. 7ª ed. Salvador: Juspodvm, 2015

O direito à vida privada é um direito inerente à pessoa humana, cuja proteção também se projeta no plano internacional, como se pode verificar no artigo 12 na Declaração Universal dos Direitos Humanos, que dispõe "ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei".

Com isso, verifica-se que a vida privada – diretamente ligada à proteção aos dados pessoais – constitui um verdadeiro direito humano e tem proteção não só nas leis infraconstitucionais, mas também constitucionais e, ainda, internacionais.

Da mesma forma acontece com a proteção aos dados pessoais da pessoa humana, vez que é diretamente ligada à vida privada e, portanto, também está guarnecida da tutela nas três esferas: infraconstitucional, constitucional e no direito internacional dos direitos humanos.

Assim, pode-se dizer que há uma proteção multinível do direito à privacidade e, consequentemente, dos dados pessoais da pessoa humana, os tornando verdadeiros direitos humanos.

Se a proteção ao direito à vida privada está diretamente ligada à proteção dos dados pessoais, e sendo a pessoa humana a única que detém o poder de permitir ou não o manuseio dos seus dados, não há como desvincular estas prerrogativas da pessoa humana, uma vez que são direitos inerente ao direito de personalidade dos indivíduos.

Neste compasso, Fernandes [5] afirma que "a divulgação de erro e/ou dificuldades acaba por inibir ou aniquilar os esforços de autossuperação, razão pela qual a esfera da privacidade", logo dos dados pessoais, "visa a fornecer um ambiente de tranquilidade emocional fundamental para uma autoavaliação de metas e objetivos pessoais".

É exatamente por esta razão que a Lei Geral de Proteção de Dados estabeleceu, em seu art. 7º, o consentimento como uma das formas que permite o manuseio dos dados pessoais alheios.

---

[5] FERNANDES, Bernardo Gonçalves. Curso de Direito Constitucional. 7ª ed. Salvador: Juspodvm, 2015

Portanto, a pessoa humana tem garantido o direito a autorizar, ou não, nas hipóteses em que seja exigido, o tratamento dos próprios dados pessoais, por força das normas infraconstitucionais, constitucionais e supranacionais, devendo as corporações assegurarem esta prerrogativa desde o princípio.

Dessa forma, a proteção multinível da privacidade e, sobretudo, dos dados pessoais, está garantida nas leis infraconstitucionais, na própria Constituição da República e, ainda, tem a tutela no direito internacional dos direitos humanos, devendo as empresas, sejam ela públicas ou privadas, garantir a aplicabilidade destas normas desde o princípio.

CONCLUSÃO

Os direitos da personalidade, tais como privacidade, intimidade, honra e imagem são tutelados tanto no plano infraconstitucional, pela Parte Geral do Código Civil de 2002 e pelos arts. 7º e 8º da Lei do Marco Civil da Internet de 2014, quanto nos direitos fundamentais do art. 5º, especificadamente nos incisos X, da Constituição da República, estando direta e intimamente ligados à proteção aos dados pessoais dos indivíduos, mesmo quando estamos tratando dos dados digitais destas pessoas, conforme consignado no art. 5º, LXXIX, pois se trata do direito humano de se ter prerrogativa em gerir os direitos inerentes à vida, à liberdade, à igualdade, à segurança e à propriedade destas pessoas físicas.

Por privacidade, entende-se que é o direito do indivíduo de realizar o controle do que veicular ou não sobre as próprias informações, direito este que está diretamente ligado à proteção de dados pessoais, uma vez que esta é exatamente a finalidade da Lei nº 13.709 de 14 de agosto de 2018, mais conhecida como a Lei Geral de Proteção de Dados – LGPD.

A LGPD trouxe uma proteção específica aos dados pessoais dos indivíduos para que tomem conhecimento de todas as operações que envolvam o tratamento ou armazenamento dos dados dentro das corporações, sejam elas públicas ou privadas, alcançando desde as empresas sem fins lucrativos, as individuais, as pequenas, médias e grandes empresas até as multinacionais.

Neste sentido, a Lei nº 12.965 de 2014, conhecida como Lei do Marco Civil da Internet, veio abranger a aplicabilidade tanto do direito à privacidade quanto a proteção aos dados pessoais ao tratar sobre os direitos e deveres dos internautas na navegação, com o intuito de proteger os dados pessoais e a privacidade dos usuários.

Neste compasso, a Constituição da República de 1988 também previu expressamente a proteção dos direitos fundamentais à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas e, ainda, dos dados pessoais.

Além disso, a proteção da privacidade e, consequentemente dos dados pessoais, são expressões dos direitos humanos desde 1948, com a Declaração Universal de Direitos Humanos, que tutela a vida privada no plano internacional por meio do artigo 12.

Com isso, tanto o direito à vida privada quanto a proteção dos dados pessoais gozam de tutela infraconstitucional, constitucional e supranacional, resultando, assim em uma proteção multinível destes direitos.

É justamente por esta razão que a pessoa humana que trabalha deve sempre ter garantido o direito a autorizar, ou não, nas hipóteses em que seja exigido, o tratamento dos próprios dados pessoais, por força das normas infraconstitucionais, constitucionais e supranacionais, devendo a empresa assegurar esta prerrogativa desde o princípio.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. [Constituição de (1988)]. **Constituição da República Federativa do Brasil**. Brasília, DF: Presidência da República, [2020]. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 14.dez. 2020.

BRASIL. **Lei nº 10.406 de 10 de janeiro de 2002.** Institui o Código Civil. Brasília, DF: Presidência da República, [2020]. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D10088.htm#art5>. Acesso em: 14.dez.2020.

BRASIL. **Lei nº 13.709 de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2020]. Disponível em:

<http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm>. Acesso em: 14.dez.2020.

BRASIL. **Lei nº 12.965 de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, [2020]. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 14.dez.2020.

COUTINHO, Aldacy Rachid. Proteção de dados do trabalhador e a questão do necessário consentimento: uma abordagem a partir da Lei n. 13.709/2018. In: **Futuro do trabalho: os efeitos da revolução digital na sociedade**. CARELLI, Rodrigo de Lacerda; CAVALCANTI, Tiago Muniz, FONSECA, Vanessa Patriota da (Org.). Brasília: ESMPU, 2020.

DINIZ, Maria Helena. **Curso de direito civil brasileiro**. Teoria do direito civil. 29ª ed. São Paulo: Saraiva, 2012.

DONEDA, Danilo. **Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade.** Disponível em: <https://www.academia.edu/23345532/Considera%C3%A7%C3%B5es_iniciais_sobre_os_bancos_de_dados_informatizados_eo_direito_%C3%A0_privacidade>. Acesso em: 13.dez.2020.

FERNANDES, Bernardo Gonçalves. **Curso de Direito Constitucional**. 7ª ed. Salvador: Juspodvm, 2015.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos.** 1948. Rio de Janeiro: UNICRIO, 2009. Disponível em: https://nacoesunidas.org/wp-content/uploads/2018/10/DUDH.pdf. Acesso em 15.dez.2020.

PARTE 2 – TRABALHOS DO DANILO DONEDA

10. PROTEÇÃO DOS DADOS PESSOAIS COMO UM DIREITO FUNDAMENTAL[1]

https://doi.org/10.36592/9786554600798-10

Danilo Doneda

RESUMO

O tratamento de dados pessoais, em particular por processos automatizados, é uma atividade de risco. A possibilidade de controle unificado das diversas atividades da pessoa, nas múltiplas situações de vida, permite o conhecimento de sua conduta pública e privada, até nos mínimos detalhes. Este artigo analisa os contornos jurídicos das informações pessoais e dos bancos de dados e explora suas principais definições no direito interno e internacional, a fim de identificar os princípios mais aparentes de uma tendência de consideração da proteção de dados pessoais como direito fundamental. A principal conclusão é que apenas sob o paradigma da interceptação, da escuta, do grampo - situações que são apenas uma parcela dos problemas que podem ocorrer no tratamento de dados com a utilização das novas tecnologias – não é possível proporcionar uma tutela efetiva aos dados pessoais na amplitude que a importância do tema hoje merece.
Palavras-chave: Direitos fundamentais. Dados pessoais. Privacidade.

Introdução

A utilização sempre mais ampla de dados pessoais para as mais variadas atividades – identificação, classificação, autorização e tantas outras – torna tais dados elementos essenciais para que a pessoa possa se mover com autonomia e liberdade nos corredores do que hoje costumamos denominar de Sociedade da In- formação[2]. Os dados pessoais chegam a fazer às vezes da própria pessoa em uma série de circunstâncias nas quais a sua presença física seria outrora indispensável. O tratamento de dados pessoais, em particular por processos automatizados, é, no entanto, uma atividade de risco. Risco que se concretiza na possibilidade de exposição e utilização indevida ou abusiva de dados pessoais, na

---

[1] Artigo originalmente publicado em Espaço Jurídico Journal of Law [EJJL], 12(2), 91–108. Disponível em: https://periodicos.unoesc.edu.br/espacojuridico/article/view/1315 Acesso em 01 de novembro de 2023.

[2] Sobre a expressão “sociedade da informação”, v. Lyon (1998, p. 384-402); v. Tb. Castells (1999).

eventualidade desses dados não serem corretos e representarem erroneamente seu titular, em sua utilização por terceiros sem o conhecimento deste, somente para citar algumas hipóteses reais. Daí resulta ser necessária a instituição de mecanismos que possibilitem à pessoa deter conhecimento e controle sobre seus próprios dados – que, no fundo, são expressão direta de sua própria personalidade. Por este motivo, a proteção de dados pessoais é considerada em diversos ordenamentos jurídicos como um instrumento essencial para a proteção da pessoa humana e como um direito fundamental.

Bancos de dados

A ferramenta que possibilita a sistematização de volumes que podem chegar a ser gigantescos de informação e que teve seu potencial exponencialmente incrementado com o advento da informática foi, propriamente, o banco de dados. Bancos de dados são, em sua acepção fundamental, um conjunto de informações estruturado de acordo com uma determinada lógica – e esta lógica é sempre uma lógica utilitarista, uma lógica que procura proporcionar a extração do máximo de proveito possível a partir de um conjunto de informações. Sabe-se há um bom tempo que a informação pode gerar proveito, como resulta claro ao verificar que é milenar a prática de coleta sistematizada de informações por alguma modalidade de censo populacional, instrumento de imensa serventia para governantes de qualquer época – a ponto de os registros históricos a respeito não serem poucos.[3]

A informação, em si, está ligada a uma série de fenômenos que cresceram em importância e complexidade de forma marcante nas últimas décadas. O que hoje a destaca de seu significado histórico é uma maior desenvoltura na sua manipulação, desde a coleta e tratamento até a comunicação da informação. Aumentando-se a capacidade de armazenamento e comunicação de informações, cresce também a variedade de formas pelas quais ela pode ser apropriada ou utilizada. Sendo maior sua maleabilidade e utilidade, mais e mais ela se torna em

[3] Desde o censo solicitado pelo imperador Yao na China de 2238 a.C., o de Moisés em 1700 a.C., passando pelo famoso censo ordenado por Augusto e mencionado pelo Evangelho de Lucas.

elemento fundamental de um crescente número de relações e aumenta sua possibilidade de influir em nosso cotidiano[4], em um crescente que tem como pano de fundo a evolução tecnológica e, especificamente, a utilização de computadores para o tratamento de dados pessoais[5] – conforme notou Stefano Rodotà ainda em 1973, "[...] a novidade fundamental introduzida pelos computadores é a transformação de informação dispersa em informação organizada."[6]

Os bancos de dados que contêm dados pessoais, tão comuns em nossos dias, proporcionam uma nova definição dos poderes e direitos a respeito das informações pessoais e, consequentemente, sobre a própria pessoa. Aumenta o número de sujeitos que podem ter acesso a um conjunto sempre mais detalhado e preciso de informações sobre terceiros, o que faz com que o estatuto jurídico desses dados se torne um dos pontos centrais que vão definir a própria autonomia, identidade e liberdade do cidadão contemporâneo.

Informação e dados pessoais

A informação pessoal, aqui tratada, deve observar certos requisitos para sua caracterização. Determinada informação pode possuir um vínculo objetivo com uma pessoa, revelando algo sobre ela. Este vínculo significa que a informação se refere às características ou ações desta pessoa, que podem ser atribuídas a ela em conformidade à lei, como no caso do nome civil ou do domicílio, ou então que são informações provenientes de seus atos, como os dados referentes ao seu consumo, informações referentes às suas manifestações, como sobre opiniões que manifesta e tantas outras. É importante estabelecer esse vínculo objetivo, pois ele afasta outras categorias de informações que, embora também possam ter alguma relação com uma pessoa, não seriam propriamente informações pessoais: as opiniões alheias sobre esta pessoa, por exemplo, a princípio não possuem esse

[4] "La informazione come servizio postula l'informazione come bene. L'assenza di tutela degli investimenti nel settore significherebbe creare una zona franca dominata da un precario parassitismo, con grave danno sia per le imprese sia per l'intero sistema, anche istituzionale, che fa perno sulla partecipazione informata." Perlingieri (1990, p. 329).
[5] Limberger (2007, p. 58 ss.).
[6] Rodotà (1973, p. 14).

vínculo objeto; também a produção intelectual de uma pessoa, em si considerada, não é per se informação pessoal (embora o fato de sua autoria o seja). Podemos concordar com Pierre Catala, que identifica uma informação pessoal quando o objeto da informação é a própria pessoa:

> Mesmo que a pessoa em questão não seja a "autora" da informa- ção, no sentido de sua concepção, ela é a titular legítima de seus elementos. Seu vínculo com o indivíduo é por demais estreito para que pudesse ser de outra forma. Quando o objeto dos dados é um sujeito de direito, a informação é um atributo da personalidade.[7]

O Conselho Europeu, por meio da Convenção de Strasbourg, de 1981, ofereceu uma definição que condiz com essa ordem conceitual. Nela, informação pessoal é "qualquer informação relativa a uma pessoa singular identificada ou susceptível de identificação."[8] É explícito, portanto, o mecanismo pelo qual é possível caracterizar uma determinada informação como pessoal: o fato de estar vinculada a uma pessoa, revelando algum aspecto objetivo desta.

Em relação à utilização dos termos "dado" e "informação", vale uma especificação. O conteúdo de ambos se sobrepõe em várias circunstâncias, o que justifica certa promiscuidade na sua utilização. Ambos os termos servem para representar um fato, determinado aspecto de uma realidade. Não obstante, cada um carrega um peso particular a ser considerado.

Assim, o "dado" apresenta conotação um pouco mais primitiva e fragmentada, como observamos em um autor que o entende como uma informação em estado potencial, antes de ser transmitida,[9] o dado estaria associado a uma espécie de "pré-informação", anterior à interpretação e ao processo de elaboração. A informação, por sua vez, alude a algo além da representação contida no dado, chegando ao limiar da cognição. Sem aludir ao seu significado ou conteúdo em si, na informação já se pressupõe uma fase inicial de depuração de seu conteúdo – daí que a informação

---

[7] Catala (1983, p. 20).
[8] Convenção nº 108 – Convenção para a proteção das pessoas em relação ao tratamento automatizado de dados pessoais, art. 2º.
[9] Wacks (1989, p. 25).

carrega também um sentido instrumental, no sentido da redução de um estado de incerteza. A doutrina não raro trata estes dois termos – dado e informação – indistintamente, ou então, procede a uma diferenciação algo empírica que merece ao menos ser ressaltada.

Deve-se lembrar ainda que o termo "informação" presta-se igualmente em certos contextos a representar diversas ordens de valores. Assim, a "liberdade de informação" como fundamento de uma imprensa livre, bem como seu correspectivo "direito à informação" [10] podem possuir conteúdo específico e que é mais remotamente relacionado ao tema deste artigo, como no caso do dever de informação pré-contratual do Código de Defesa do Consumidor.

A informação pessoal está, quase como ato reflexo, ligada à privacidade por uma equação simples e básica que associa um maior grau de privacidade à menor difusão de informações pessoais e vice-versa. Esta equação nem de longe encerra toda a complexa problemática em torno dessa relação, porém pode servir como ponto de partida para ilustrar como a proteção das informações pessoais passou a encontrar guarida em nosso ordenamento jurídico: como um desdobramento da tutela do direito à privacidade.

Com o aludido aumento da importância da informação de uma forma geral, foi justamente em torno dela que a temática da privacidade passou a orbitar, em especial ao se tratar de dados pessoais.[11] Esta guinada, que acabou por plasmar o próprio conteúdo do termo privacidade, pode ser verificada com clareza nas construções legislativas e jurisprudenciais que afrontaram o tema nos últimos 40 anos, das quais algumas referências mais significativas poderiam ser a concepção de uma *informational privacy* nos Estados Unidos, cujo "núcleo duro" é composto pelo direito de acesso a dados armazenados por órgãos públicos e também pela disciplina de proteção de crédito; assim como a autodeterminação informativa estabelecida pelo Tribunal Constitucional Federal alemão[12] e a Diretiva 95/46/CE da

---

[10] Sobre o tema, v. Carvalho (1999).
[11] Sobre o tema, v. Doneda (2006).
[12] A sentença de 15 de dezembro de 1983 do Tribunal Constitucional Federal alemão consolidou a existência de um "direito à autodeterminação informativa" (informationelle selbstestimmung), que consistia no direito de um indivíduo controlar a obtenção, a titularidade, o tratamento e a transmissão de dados relativos à sua pessoa.

União Europeia (relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados), com todas as suas consequências.

O ponto fixo de referência nesse processo é que, entre os novos prismas para enquadrar a questão, mantém-se uma constante referência objetiva a uma disciplina para os dados pessoais, que manteve o nexo de continuidade com a disciplina da privacidade, da qual é uma espécie de herdeira, atualizando-a e impondo características próprias.

Por meio da proteção de dados pessoais, garantias a princípio relacionadas à privacidade passam a ser vistas em uma ótica mais abrangente, pela qual outros interesses devem ser considerados, abrangendo as diversas formas de controle tornadas possíveis com a manipulação de dados pessoais. Para uma completa apreciação do problema, estes interesses devem ser considerados pelo operador do direito pelo que representam, e não somente pelo seu traço visível – a violação da privacidade. Esta vinculação do tratamento de dados pessoais com o controle foi bem caracterizada pelo Ministro Ruy Rosado de Aguiar, ainda em decisão de 1995:

> A inserção de dados pessoais do cidadão em bancos de informações tem se constituído em uma das preocupações do Estado moderno, onde o uso da informática e a possibilidade de controle unifica- do das diversas atividades da pessoa, nas múltiplas situações de vida, permitem o conhecimento de sua conduta pública e privada, até nos mínimos detalhes, podendo chegar à devassa de atos pessoais, invadindo área que deveria ficar restrita à sua intimidade; ao mesmo tempo, o cidadão objeto dessa indiscriminada colheita de informações, muitas vezes, sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo. E assim como o conjunto dessas informações pode ser usado para fins lícitos, públicos e privados, na prevenção ou repressão de delitos, ou habilitando o particular a celebrar contratos com pleno conhecimento de causa, também pode servir, ao Estado ou ao particular, para alcançar fins contrários à moral ou ao Direito, como instrumento de perseguição política ou opressão econômica. A importância do tema cresce de ponto quando se observa o número imenso de atos da vida

humana praticados através da mídia eletrônica ou registrados nos disquetes de computador.[13]

Desenvolvimento das leis de proteção de dados

O tratamento autônomo da proteção de dados pessoais é uma tendência hoje fortemente enraizada em diversos ordenamentos jurídicos e é caso emblemático de uma tendência que, a princípio, parecia apenas destinada a mudar de- terminado patamar tecnológico e a solicitar previsões pontuais no ordenamento, mas que, em seus desdobramentos, veio a formar as bases para o que vem sendo tratado, hoje, como um direito fundamental à proteção de dados.[14][13] Esse desenvolvimento foi intenso nas cerca de quatro décadas que a disciplina ostenta. A mudança do enfoque dado à proteção de dados nesse período pode ser brevemente entrevista na classificação evolutiva das leis de proteção de dados pessoais realizada por Viktor Mayer-Scönberger,[15] que vislumbra quatro diferentes gerações de leis que partem desde um enfoque mais técnico e restrito até a abertura mais recente a técnicas mais amplas e condizentes com a profundidade da tecnologia adotada para o tratamento de dados, em busca de uma tutela mais eficaz e também vinculando a matéria aos direitos fundamentais.

A primeira dessas quatro gerações de leis[16] era composta por normas que refletiam estado da tecnologia e a visão do jurista à época, pretendendo regular um cenário no qual centros elaboradores de dados, de grande porte, concentrariam a coleta e gestão dos dados pessoais. O núcleo dessas leis girava em torno da concessão de autorizações para a criação desses bancos de dados e do seu controle *a posteriori* por órgãos públicos.[17] Essas leis também enfatizavam o controle do uso de informações pessoais pelo Estado e pelas suas estruturas administrativas, que eram o destinatário principal (quando não o único) dessas

---

[13] STJ, Recurso Especial n. 22.337/RS, rel. Ministro Ruy Rosado de Aguiar, DJ 20/03/1995, p. 6119.
[14] Piñar Mañas (2005, p. 19-36).
[15] Mayer-Scönberger (1997, p. 219-242).
[16] Exemplo dessas leis de primeira geração são a Lei do Land alemão de Hesse, de 1970; a primeira lei nacional de proteção de dados, sueca, que foi o Estatuto para bancos de dados de 1973 – Data Legen 289, ou Datalag, além do Privacy Act norte-americano de 1974.
[17] Sampaio (1997, p. 490).

normas. Esta primeira geração de leis vai, aproximadamente, até a *Bundesdatenschutzgesetz*, a lei federal da República Federativa da Alemanha sobre proteção de dados pessoais, de 1977.

A falta de experiência no tratamento com tecnologias ainda pouco familiares, aliada ao receio de um uso indiscriminado dessa tecnologia, sem que se soubesse ao certo suas consequências, fez com que se optasse por princípios de proteção, não raro bastante abstratos e amplos, focalizados basicamente na atividade de processamento de dados,[18] além de regras concretas e específicas dirigidas aos agentes diretamente responsáveis pelo processamento dos dados. Esse enfoque era natural, visto a motivação dessas leis ter sido a "ameaça" representada pela tecnologia e, especificamente, pelos computadores. A estrutura e a gramática de tais leis era algo tecnocrático e condicionado pela informática – nelas, tratava-se dos "bancos de dados", e não propriamente da "privacidade", desde seus princípios genéricos até os regimes de autorização e de modalidades de tratamento de dados, a serem determinados *ex ante*, sem prever a participação do cidadão neste processo.[19]

Essas leis de proteção de dados de primeira geração não demoraram muito a se tornar ultrapassadas, diante da multiplicação dos centros de processamento de dados, que inviabilizou o controle baseado em um regime de autorizações, rígido e detalhado, que demandava um minucioso acompanhamento. A segunda geração de leis sobre a matéria surgiu no final da década de 1970, já com a consciência da "diáspora" dos bancos de dados informatizados. Pode-se dizer que o seu primeiro grande exemplo foi a Lei Francesa de Proteção de Dados Pessoais de 1978, intitulada *Informatique et Libertées*, [20] além da já mencionada Bundesdatenschutzgesetz. A característica básica que diferencia tais leis das anteriores é que sua estrutura não está mais fixada em torno do fenômeno computacional em si, mas se baseia na consideração da privacidade e na proteção

---

[18] Cf. Spiros Simitis (1997, p. 565).
[19] Viktor Mayer-Scönberger. General development of data protection in Europe, cit., p. 223-224.
[20] Lei 78-17 de 6 de janeiro de 1978.

dos dados pessoais como uma liberdade negativa, a ser exercida pelo próprio cidadão (o que é patente na própria denominação da Lei Francesa).[21]

Tal evolução refletia a insatisfação de cidadãos que sofriam com a utilização por terceiros de seus dados pessoais e careciam de instrumentos para defender diretamente seus interesses. Além disso, o controle, nos moldes das leis anteriores, tornou-se inviável, dada a fragmentação dos centros de tratamento dos dados pessoais. Assim, criou-se um sistema que fornecia instrumentos para o cidadão identificar o uso indevido de suas informações pessoais e propor a sua tutela.

Estas leis apresentavam igualmente seus problemas, o que motivou uma subsequente mudança de paradigma: percebeu-se que o fornecimento de dados pessoais pelos cidadãos tinha se tornado um requisito indispensável para a sua efetiva participação na vida social. O que era exceção veio a se tornar regra. Tanto o Estado quanto os entes privados utilizavam intensamente o fluxo de informações pessoais para seu funcionamento, e a interrupção ou mesmo o questionamento deste fluxo pelo cidadão implica muito frequentemente a sua exclusão de algum aspecto da vida social. Uma terceira geração de leis, surgida na década de 1980, procurou sofisticar a tutela dos dados pessoais, que continuou centrada no cidadão, porém passou a abranger mais do que a liberdade de fornecer ou não os próprios dados pessoais, preocupando-se também em garantir a efetividade desta liberdade. A proteção de dados é vista, por tais leis, como um processo mais complexo, que envolve a própria participação do indivíduo na sociedade e considera o contexto no qual lhe é solicita- do que revele seus dados, estabelecendo meios de proteção para as ocasiões em que sua liberdade de decidir livremente é cerceada por eventuais condicionantes – proporcionando o efetivo exercício da autodeterminação informativa.

A autodeterminação informativa surgiu basicamente como uma extensão das liberdades presentes nas leis de segunda geração, e são várias as mudanças específicas nesse sentido que podem ser identificadas na estrutura dessas novas

---

[21] Como representante desta geração de leis, podemos mencionar também a Lei Austríaca (Datenschutzgesetz (DSG), Lei de 18 de outubro de 1978, n. 565/1978); além de que as constituições portuguesa e espanhola apontam nesse sentido, mesmo que as leis de proteção de dados destes países tenham surgido somente um pouco mais tarde.

leis. O tratamento dos dados pessoais era visto como um processo, que não se encerrava na simples permissão ou não da pessoa à utilização de seus dados pes soais, porém procurava incluí-la em fases sucessivas do processo de tratamento e utilização de sua própria informação por terceiros, além de compreender algumas garantias, como o dever de informação.

A autodeterminação informativa era, porém, o privilégio de uma minoria que decidia enfrentar os custos econômicos e sociais do exercício dessas prerrogativas. Verificado esse caráter exclusivista, uma quarta geração de leis de proteção de dados, como as que existem hoje em vários países, surgiu e caracterizou-se por procurar suprir as desvantagens do enfoque individual existente até então. Nestas leis procura-se enfocar o problema integral da informação, pois elas presumem que não se pode basear a tutela dos dados pessoais simplesmente na escolha individual – são necessários instrumentos que elevem o padrão coletivo de proteção.

Entre as técnicas utilizadas, essas leis procuraram fortalecer a posição da pessoa em relação às entidades que coletam e processam seus dados, reconhecendo um desequilíbrio nessa relação que não era resolvido por medidas que simples- mente reconheciam o direito à autodeterminação informativa. Outra técnica é, paradoxalmente, a própria redução do papel da decisão individual de autodeterminação informativa. Isso ocorre por conta do pressuposto de que determinadas modalidades de tratamento de dados pessoais necessitam de uma proteção no seu mais alto grau, que não pode ser conferida exclusivamente a uma decisão individual – como é o caso para certas modalidades de utilização de dados sensíveis.

Outra característica é a disseminação do modelo das autoridades independentes para a atuação da lei – tanto mais necessária com a diminuição do poder de "barganha" com o indivíduo para a autorização ao processamento de seus dados, e também o surgimento de normativas conexas na forma, por exemplo, de normas específicas para alguns setores de processamento de dados (para o setor de saúde ou de crédito ao consumo). Hoje, pode-se afirmar que um tal modelo de proteção de dados pessoais é representado pelos países europeus que transcreveram para seus ordenamentos as Diretivas europeias em matéria de

proteção de dados, em especial a já mencionada Diretiva 95/46/CE e a Diretiva 2000/58/CE (conhecida como Diretiva sobre privacidade e as comunicações eletrônicas.

Princípios de proteção de dados pessoais

A aludida "progressão generacional" das leis sobre proteção de dados pessoais faz referência, não por acaso, a uma linguagem própria da informática e exprime a lógica da busca por modelos jurídicos mais ricos e completos.[22] Não obstante essa sua marcada mudança de perfil com os anos, é possível reagrupar materialmente seus objetivos e linhas de atuação principais em torno de alguns princípios comuns, presentes em diversos graus em ordenamentos vários – no que podemos verificar uma forte manifestação da convergência das soluções legislativas quanto à matéria em diversos países, bem como uma tendência sempre mais marcada rumo à consolidação de certos princípios básicos e sua vinculação sempre mais estreita com a proteção da pessoa e com os direitos fundamentais.

Destes princípios, alguns se encontram já presentes nas leis de primeira e segunda geração, desenvolvidos pelas leis posteriores. Uma busca mais larga poderá, porém, retraçar suas origens em uma série de discussões que, na segunda metade da década de 1960, acompanhou a tentativa do estabelecimento do *National Data Center*, que consistiria basicamente em um gigantesco e jamais realizado banco de dados sobre os cidadãos norte-americanos para uso da administração federal.[23]

Após o fracasso da tentativa de instituição deste banco de dados centralizado, vários dos temas que foram levantados em meio à discussão sobre sua possibilidade continuaram a ser desenvolvidos, pois se o *National Data Center* particularmente não vingou, a realidade era que muitos outros bancos de dados

[22] Cf. Rodotà (1999, p. 103).

[23] O National Data Center foi projetado para reunir as informações sobre os cidadãos norte--americanos disponíveis em diversos órgãos da administração federal em um único banco de da- dos – a partir de um projeto original, que pretendia unificar os cadastros do Censo, dos registros trabalhistas, do fisco e da previdência social. Garfinkel (2000, p. 13). Após acirradas discussões sobre a ameaça potencial que representaria às liberdade individuais, o governo norte-america- no desistiu do projeto. V. Miller (1971).

pessoais de menor âmbito iam se estruturando. Uma das áreas na qual essa discussão ecoou com maior força foi a da saúde, pela justificada preocupação com o tratamento de dados médicos por sistemas informatizados. No início da década de 1970, a *Secretary for health, education and welfare* reuniu uma comissão de especialistas que divulgou, em 1973, um estudo que concluiu pela relação direta entre a privacidade e os tratamentos de dados pessoais, além da necessidade de estabelecer a regra do controle sobre as próprias informações:

> A privacidade pessoal de um indivíduo é afetada diretamente pelo tipo de divulgação e utilização que é feita das informações registradas a seu respeito. Um tal registro, contendo informações sobre um indivíduo identificável deve, portanto, ser administrado com procedimentos que permitam a este indivíduo ter o direito de participar na sua decisão sobre qual deve ser o conteúdo deste registro e qual a divulgação e utilização a ser feita das informações pessoais nele contida. Qualquer registro, divulgação e utilização das informações pessoais fora destes procedimentos não devem ser permitidas, por consistirem em uma prática desleal, a não ser que tal registro, utilização ou divulgação sejam autorizados por lei.[24]

Uma concepção como esta requer que sejam estabelecidos meios de garantia para o cidadão, que efetivamente vieram descritos como:

> - Não deve existir um sistema de armazenamento de informações pessoais cuja existência seja mantida em segredo.
> - Deve existir um meio para um indivíduo descobrir quais informações a seu respeito estão contidas em um registro e de qual forma ela é utilizada.
> - Deve existir um meio para um indivíduo evitar que a informação a seu respeito colhida para um determinado fim seja utilizada ou disponibilizada para outros propósitos sem o seu conhecimento.
> - Deve existir um meio para um indivíduo corrigir ou retificar um registro de informações a seu respeito.

[24] EUA (1973).

- Toda organização que estruture, mantenha, utilize ou divulgue registros com dados pessoais deve garantir a confiabilidade destes dados para os fins pretendidos e deve toar as devidas precauções para evitar o mau uso destes dados.[25]

Tais regras, de caráter marcantemente procedimental,[26] apresentaram um conjunto de medidas que passou a ser encontrado em várias normativas sobre proteção de dados pessoais, às quais se passou a referir como *Fair Information Principles*. Esse "núcleo comum" encontrou expressão como um conjunto de princípios a serem aplicados na proteção de dados pessoais principalmente com a Convenção de Strasbourg[27] e nas Guidelines da OCDE,[28] no início da década de 1980. É possível elaborar uma síntese destes princípios:[29]

a) Princípio da publicidade (ou da transparência), pelo qual a existência de um banco de dados com dados pessoais deve ser de conhecimento público, seja por meio da exigência de autorização prévia para funcionar, da notificação a uma autoridade sobre sua existência, ou do envio de relatórios periódicos;
b) Princípio da exatidão: os dados armazenados devem ser fiéis à realidade, o que compreende a necessidade de que sua coleta e seu tratamento sejam feitos com cuidado e correção, e de que sejam realizadas atualizações periódicas conforme a necessidade;
c) Princípio da finalidade, pelo qual qualquer utilização dos dados pessoais deve obedecer à finalidade comunicada ao interessado antes da coleta de seus dados. Este princípio possui grande relevância prática: com base nele fundamenta-se a restrição da transferência de dados pessoais a terceiros, além do que se pode, a

---

[25] Idem
[26] Assim enquadrariam-se com maior facilidade no espírito da cláusula do *due process* norte-americano. Bennett (1992, p. 98).
[27] Convenção nº 108 do Conselho Europeu – Convenção para a proteção das pessoas em relação ao tratamento automatizado de dados pessoais.
[28] Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, disponível em: <www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html>. Estes princípios seriam: (1) collection limitation principle; (2) data limitation principle; (3) purpose specification principle; (4) use limitation principle; (5) security safeguard principle; (6) openness principle; (7) individual participation principle. Wuermeling (1996, p. 416).
[29] Cf. Stefano Rodotà. Repertorio di fine secolo, cit. p. 62. José Adércio L. Sampaio. Direito à intimidade e à vida privada. cit., p. 509 ss.

> partir dele, estruturar-se um critério para valorar a razoabilidade da utilização de determinados dados para certa finalidade (fora da qual haveria abusividade);
> d) Princípio do livre acesso, pelo qual o indivíduo tem acesso ao banco de dados no qual suas informações estão armazenadas, podendo obter cópias desses registros, com a consequente possibilidade de controle desses dados; após este acesso e de acordo com o princípio da exatidão, as informações incorretas poderão ser corrigidas e aquelas obsoletas ou impertinentes poderão ser suprimidas, ou mesmo pode-se proceder a eventuais acréscimos;
> e) Princípio da segurança física e lógica, pelo qual os dados devem ser protegidos contra os riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado.

Estes princípios, mesmo que fracionados, condensados ou adaptados, formam a espinha dorsal das diversas leis, tratados, convenções ou acordos entre privados em matéria de proteção de dados pessoais, formando o núcleo das questões com as quais o ordenamento deve se deparar ao procurar fornecer sua própria solução ao problema da proteção dos dados pessoais.

A aplicação de tais princípios, no entanto, é a parte mais aparente de uma tendência rumo à constatação da autonomia da proteção de dados pessoais e à sua consideração como um direito fundamental em diversos ordenamentos. Alguns países que sofreram uma mudança de regime político que lhes proporcionou a re- elaboração de suas cartas fundamentais foram os primeiros nos quais foi possível observar uma tendência à consideração da problemática relacionada à informática e à informação pessoal em nível constitucional. Nesse sentido, nas Constituições da Espanha [30] e de Portugal [31] se encontram

[30] A Constituição Espanhola de 1978 contém os seguintes dispositivos:
Art. 18. – [...] 4. La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos. [...] Art. 105. – [...] b) La Ley regulará el acceso de los ciudadanos a los archivios y registros ad- ministrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas.

[31] A Constituição Portuguesa de 1976 dispõe sobre a utilização da informática nos sete incisos de seu artigo 35:
“Artigo 35. (Utilização da informática)
1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua rectificação e actualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.

dispositivos destinados a afrontar os problemas da utilização da informática, e, no caso da Constituição portuguesa, uma referência explícita à proteção de dados pessoais.

É possível considerar a Convenção de Strasbourg como o principal marco de uma abordagem da matéria pela chave dos direitos fundamentais. Em seu preâmbulo, a convenção deixa claro que a proteção de dados pessoais está diretamente ligada à proteção dos direitos humanos e das liberdades fundamentais, entendendo-a como pressuposto do estado democrático e trazendo para este campo a disciplina, evidenciando sua deferência ao artigo 8º da Convenção Europeia para os Direitos do Homem.[32] Posteriormente, também transparece, com clareza, presença dos direitos fundamentais na Diretiva 95/46/CE sobre proteção de dados pessoais na União Europeia.[33] Seu artigo 1º, que trata do "objetivo da diretiva", afirma que "Os Estados-membros assegurarão, em conformidade com a presente directiva, a protecção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao trata- mento de dados pessoais."

2.A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua protecção, designadamente através de entidade administrativa independente.
3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosó- fica ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis.
4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excepcionais previstos na lei.
5. É proibida a atribuição de um número nacional único aos cidadãos.
6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de protecção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional.
7. Os dados pessoais constantes de ficheiros manuais gozam de protecção idêntica à prevista nos números anteriores, nos termos da lei."

[32] Cujo teor é o seguinte:
1- Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.
2- Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade demo- crática, seja necessária para a segurança nacional, para a segurança pública, para o bem estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros."

[33] Mencione-se, de passagem, que a expressão "direitos fundamentais" é evocada por seis vezes nas considerações iniciais da Diretiva.

O documento europeu que levou mais adiante essa sistemática foi, certamente, a Carta dos Direitos Fundamentais da União Europeia, proclamada em 7 de dezembro de 2000. Seu artigo 8º, que trata da "proteção de dados pessoais", inspira-se no artigo 8º da Convenção de Strasbourg, na Diretiva 95/46/CE e no artigo 286º do tratado instituidor da União Europeia.[34] Não obstante, nota-se um duplo matiz: se a Diretiva, por um lado, procura proteger a pessoa física em relação ao tratamento de seus dados pessoais, por outro se destaca sua missão de induzir o comércio mediante o estabelecimento de regras comuns para proteção de dados na região, o que não surpreende se considerarmos as exigências de um mercado unificado como o europeu em diminuir de forma ampla os custos de transações, o que inclui harmonizar as regras relativas a dados pessoais.[35]

Proteção de dados no ordenamento brasileiro

No panorama do ordenamento brasileiro, o reconhecimento da proteção de dados como um direito autônomo e fundamental não deriva de uma dicção explícita e literal, porém da consideração dos riscos que o tratamento automatizado traz à proteção da personalidade à luz das garantias constitucionais de igualdade substancial, liberdade e dignidade da pessoa humana, juntamente com a proteção da intimidade e da vida privada.

A bem da verdade, pode-se encontrar uma menção ao caráter de direito fundamental da proteção de dados pessoais na Declaração de Santa Cruz de La Sierra, documento final da XIII Cumbre Ibero-Americana de Chefes de Estado e

[34] De seguinte teor:
"Artigo 286º.
1. A partir de 1 de Janeiro de 1999, os actos comunitários relativos à protecção das pessoas singulares em matéria de tratamento de dados de carácter pessoal e de livre circulação desses dados serão aplicáveis às instituições e órgãos instituídos pelo presente Tratado, ou com base nele.
2. Antes da data prevista no no. 1, o Conselho, deliberando nos termos do artigo 251o., criará um órgão independente de supervisão, incumbido de fiscalizar a aplicação dos citados "actos comunitários às instituições e órgãos da Comunidade e adoptará as demais disposições que se afigurem adequadas".
[35] Este caráter levou alguns autores a desencorajarem a leitura da diretiva em chave de direitos fundamentais do homem em relação à informação pessoal, apesar de reconhecerem que, "*dal punto di vista più genuinamente privatistico, non v'è dubbio che la direttiva [...] sia destinata a diventare un punto di riferimento fondamentale nella ricostruzione sistematica dei diritti della personalità, almeno nella misura in cui il concetto di personalità si trovi a far i conti con la real- tà informatica e telematica*". v. Francesco Macario." (MACARIO, 1997, p. 8-9).

de Governo, firmada pelo Governo Brasileiro em 15 de novembro de 2003. No item 45 da referida Declaração lê-se que:

> Estamos também conscientes de que a protecção de dados pessoais é um direito fundamental das pessoas e destacamos a importância das iniciativas reguladoras ibero-americanas para proteger a privacidade dos cidadãos, contidas na Declaração de Antigua, pela qual se cria a Rede Ibero-Americana de Protecção de Dados, aberta a todos os países da nossa Comunidade.

A proteção de dados pessoais no ordenamento brasileiro não se estrutura a partir de um complexo normativo unitário. A Constituição Brasileira contempla o problema da informação inicialmente por meio das garantias à liberdade de expressão [36] e do direito à informação, [37] que deverão eventualmente ser confrontados com a proteção da personalidade e, em especial, com o direito à privacidade. Além disso, a Constituição considera invioláveis a vida privada e a intimidade (art. 5º, X), veja-se especificamente a interceptação de comunicações tele- fônicas, telegráficas ou de dados (artigo 5º, XII), bem como instituiu a ação de habeas data (art. 5º, LXXII), que basicamente estabelece uma modalidade de direito de acesso e retificação dos dados pessoais. Na legislação infraconstitucional, destaque-se o Código de Defesa do Consumidor, Lei 8.078/90, cujo artigo 43 estabelece uma série de direitos e garantias para o consumidor em relação às suas in- formações pessoais presentes em "bancos de dados e cadastros", implementando uma sistemática baseada nos *Fair Information Principles* à matéria de concessão de crédito e possibilitando que parte da doutrina verifique neste texto legal o mar- co normativo dos princípios de proteção de dados pessoais no direito brasileiro.[38]

---

[36] Constituição Brasileira, art. 5º, IX; art. 220.
[37] Constituição Brasileira, art. 5º, XIV; art. 220; incluindo o direito ao recebimento de informa- ções de interesse coletivo ou particular dos órgãos públicos (art. 5º, XXXIII), bem como o direito à obtenção de certidões de repartições públicas (art. 5º, XXXIV).
[38] Cf. Carvalho (2003, p. 77-119).

O habeas data, instituto que no direito brasileiro tem a forma de uma ação constitucional, foi introduzido pela Constituição de 1988.[39] Com um *nomen iuris* original, introduziu em nosso ordenamento o direito de acesso, carregando consigo algo da carga semântica do habeas corpus. A sua influência em outras legislações latino-americanas chegou a provocar a discussão sobre a existência de um modelo de proteção de dados que circule dentro do subcontinente.[40]

Cabe ressaltar que o habeas data brasileiro surgiu basicamente como um instrumento para a requisição das informações pessoais em posse do poder público, em particular dos órgãos responsáveis pela repressão durante o regime militar e sem maiores vínculos, portanto, com uma eventual influência da experiência europeia ou norte--americana relativa à proteção de dados pessoais, já em pleno desenvolvimento à época.

Posteriormente o habeas data foi regulamentado pela Lei 9.507, de 1997. A ação de habeas data visa a assegurar um direito presente em nosso ordenamento jurídico, ainda que não expresso literalmente. Por meio dela, o cidadão pode acessar e retificar seus dados pessoais em bancos de dados "de entidades governamentais ou de caráter público" (posteriormente ampliou-se o sentido deste "caráter público", incluindo-se os bancos de dados referentes a consumidores, mesmo que administra- dos por privados). A ação não é acompanhada, porém, de instrumentos que possam torná-la ágil e eficaz o suficiente para a garantia fundamental de proteção dos dados pessoais: além do seu perfil estar demasiadamente associado à proteção de liberdades negativas, algo que se percebe em vários dos seus pontos estruturais, como a necessidade de sua interposição por meio de advogado ou então a necessidade de demonstração de recusa de fornecimento dos dados por parte do administrador de banco de dados, ela é, substancialmente, um instrumento que proporciona uma tu- tela completamente anacrônica e ineficaz à realidade das comunicações e tratamentos de dados pessoais na Sociedade da Informação. Não surpreende, portanto, que desde certo tempo a doutrina brasileira tenha assumido

[39] Constituição Federal, art. 5º, LXXII: "Conceder-se-á habeas data: a) para assegurar o conhecimento de informações relativas à pes- soa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo."

[40] Sobre o tema, Puccinelli (1999).

posição majoritariamente crítica em relação à ação, tratando-a ora como "um remédio de valia, no fundo, essencialmente simbólica", para Luís Roberto Barroso,[41] ora como "uma ação voltada para o passado", para Dalmo de Abreu Dallari.[42]

Parece existir no direito brasileiro, de forma generalizada, uma consciência de que seria possível tratar de forma satisfatória os problemas relacionados às informações pessoais em bancos de dados a partir de uma série de categorizações, geralmente generalistas e algo abstratas: sobre o caráter rigidamente público ou particular de uma espécie de informação; a respeito da característica sigilosa ou não de determinada comunicação, e assim por diante. Enfim: com um sistema baseado em etiquetas, permissões ou proibições para o uso de informações específicas, sem considerar os riscos objetivos potencializados pelo tratamento informatizado das informações pessoais.

Uma determinada leitura da sistemática da Constituição Brasileira parece encorajar essa perspectiva. Nela, a proteção da privacidade (por intermédio da menção à inviolabilidade da intimidade e da vida privada) encontra-se em um dispositivo (art. 5º, X), enquanto que outro dispositivo se refere à inviolabilidade do "sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas." (art. 5º, XII).

Tal técnica legislativa acabou por fundamentar uma interpretação no míni- mo temerosa no que diz respeito à matéria: se, por um lado, a privacidade é encarada como um direito fundamental, as informações pessoais em si parecem, a uma parte da doutrina, serem protegidas somente em relação à sua "comunicação", conforme o art. 5o, XII, que trata da inviolabilidade da comunicação de dados.

Tal interpretação, além de dissonante com a visão segundo a qual privacidade e informações pessoais são temas sempre mais relacionados e, em muitas ocasiões, quase que indistinguíveis entre si – conforme atesta o mencionado desenvolvimento de leis que tratam da proteção de dados pessoais e também os documentos transnacionais que associam o caráter de direito fundamental à proteção de dados pessoais –, traz consigo o enorme risco de acabar por se tornar uma norma que sugere uma grande permissividade em relação à utilização de informações pessoais.

---

[41] Barroso (1998, p. 212).
[42] Dallari (1997, p. 100).

Nesse sentido, recentemente, uma decisão do STF, relatada pelo Ministro Sepúlveda Pertence, reconheceu expressamente a inexistência de uma garantia de inviolabilidade sobre dados armazenados em computador com fulcro em garantias constitucionais, endossando tese de Tércio Sampaio Ferraz Júnior, segundo a qual o ordenamento brasileiro tutelaria o sigilo das comunicações – e não dos dados em si.[43] Nesta decisão fica saliente a dificuldade em tratar do tema da informação pessoal de forma diversa daquela binária – sigilo/abertura, público/privado– de forma que reflita a complexidade da matéria da informação.

A leitura das garantias constitucionais para os dados somente sob o prisma de sua comunicação e de sua eventual interceptação lastreia-se em uma interpretação que não chega a abranger a complexidade do fenômeno da informação ao qual fizemos referência. Há um hiato que segrega a tutela da privacidade, esta constitucionalmente protegida, da tutela das informações pessoais em si – que, para a cor- rente mencionada, gozariam de uma proteção mais tênue. E este hiato possibilita a perigosa interpretação que pode eximir o aplicador de considerar os casos nos quais uma pessoa é ofendida em sua privacidade – ou tem outros direitos

---

[43] "Em primeiro lugar, a expressão 'dados' manifesta uma certa impropriedade (BASTOS; GAN- DRA, 1989, p. 73). Os citados autores reconhecem que por "dados" não se entende o objeto de comunicação, mas uma modalidade tecnológica de comunicação. Clara, nesse sentido, a observação de Manoel Gonçalves Ferreira Filho (1990, p. 38).— "Sigilo de dados. O direito anterior não fazia referência a essa hipótese. Ela veio a ser prevista, sem dúvida, em decorrência do desenvolvimento da informática. Os dados aqui são os dados informáticos (v. incs. XIV e LXXII)." A interpretação faz sentido. O sigilo, no inciso XII do art. 5º, está referido à comunicação, no interesse da defesa da privacidade. Isso é feito, no texto, em dois blocos: a Constituição fala em sigilo "da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas." Note-se, para a caracterização dos blocos, que a conjunção e uma correspondência com telegrafia, segue-se uma vírgula e depois, a conjunção de dados com comunicações telefônicas. Há uma simetria nos dois blocos. Obviamente o que se regula é comunicação por correspondência e telegrafia, comunicação de dados e telefônica. O que fere a liberdade de omitir pensamento é, pois, entrar na comunicação alheia, fazendo com que o que deveria ficar entre sujeitos que se comunicam privadamente passe ilegitimamente ao domínio de um terceiro. Se alguém elabora para si um cadastro sobre certas pessoas, com informações marcadas por avaliações negativas, e o torna público, poderá estar cometendo difamação, mas não quebra sigilo de dados. Se estes dados, armazenados eletronicamente, são transmitidos, privadamente, a um parceiro, em relações mercadológicas, para defesa do mercado, também não está havendo quebra de sigilo. Mas, se alguém entra nessa transmissão como um terceiro que nada tem a ver com a relação comunicativa, ou por ato próprio ou porque uma das partes lhe cede o acesso indevidamente, estará violado o sigilo de dados. A distinção é decisiva: o objeto protegido no direito à inviolabilidade do sigilo não são os dados em si, mas a sua comunicação restringida (liberdade de negação). A troca de informações (comunicação) privativa é que não pode ser violada por sujeito estranho à comunicação. Doutro modo, se alguém, não por razões profissionais, ficasse sabendo legitima- mente de dados incriminadores relativos a uma pessoa, ficaria impedido de cumprir o seu dever de denunciá-lo! (FERRAZ JÚNIOR, 1993, p. 447).

fundamentais desrespeitados – não de forma direta, porém por meio da utilização abusiva de suas informações pessoais em bancos de dados. Não é necessário ressaltar novamente o quanto hoje em dias as pessoas são reconhecidas em diversos relacionamentos não de forma direta, mas mediante a representação de sua personalidade, fornecida pelos seus dados pessoais, aprofundando ainda mais a íntima relação entre tais dados e a própria identidade e personalidade de cada um de nós.

Apenas sob o paradigma da interceptação, da escuta, do grampo – situações que são apenas uma parcela dos problemas que podem ocorrer no tratamento de da- dos com a utilização das novas tecnologias – não é possível proporcionar uma tutela efetiva aos dados pessoais na amplitude que a importância do tema hoje merece.

O esforço a ser empreendido pela doutrina e pela jurisprudência seria, em nosso ponto de vista, basicamente o favorecimento de uma interpretação dos incisos X e XII do art. 5º mais fiel ao nosso tempo, ou seja, reconhecendo a íntima ligação que passam a ostentar os direitos relacionados à privacidade e à comunicação de dados. Desta forma, seria dado o passo necessário à integração da personalidade em sua acepção mais completa na vicissitudes da Sociedade da Informação.

REFERÊNCIAS

BARROSO, Luís Roberto. Viagem redonda: habeas data, direitos constitucionais e provas ilícitas. In: WAMBIER, Teresa Arruda Alvim (Coord.). Habeas data.São Paulo: RT, 1998.

BENNETT, Colin. Regulating privacy. Data protection and public policy in Eu- rope and UnitedStates. Itahaca: Cornell University Press, 1992.

BRASIL. Constituição: República Federativa do Brasil de 1988. Brasília, DF: Senado Federal, 1988.

BRASIL. Superior Tribunal de Justiça. Recurso Especial n. 22.337/RS. Relator: Ministro Ruy Rosado de Aguiar. Diário da Justiça, Brasília, DF, 20 mar. 1995.

CASTELLS, Manuel. A sociedade em rede (A era da informação, economia, so- ciedade e cultura). São Paulo: Paz e Terra, 1999. v. 1.

CARVALHO, Ana Paula Gambogi. O consumidor e o direito à autodetermina- ção informacional. Revista de Direito do Consumidor, n. 46, p. 77-119, abr./jun. 2003.

CARVALHO, Luis Gustavo Grandinetti de. Direito de Informação e Liberdade de Expressão. Rio de Janeiro: Renovar, 1999.

CATALA, Pierre. Ebauche d' une théorie juridique de l'information. Informatica e Dirito, ano 9, p. 20, janv./avril 1983.

DALLARI, Dalmo de Abreu. O habeas data no sistema jurídico brasileiro. Revis- ta de la Faculdade de derecho de La Pontifícia Universidade Católica del Peru,n. 51, p. 100, 1997.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006.

EUA. Records, computers and the rights of citizens. Reporto f the Secretary's Advisory Committee on Automated Personal Data Systems, 1973. Disponível em: <aspe.hhs.gov/datacncl/1973privacy/c3.htm>.

FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. Revista da Faculdade de Direito da Universidade de São Paulo. 1993. v. 88.

GARFINKEL, Simson. Database nation. Sebastopol: O'Reillly, 2000.

LIMBERGER, Têmis. O direito à intimidade na era da informática. Porto Ale- gre: Livraria do Advogado, 2007.

LYON, David. The roots of the information society Idea. In: O'SULLIVAN, Tim; JEWKES, Yvonne (Ed.). The media studies reader. London: Arnold, 1998.

MACARIO, Francesco. La protezione dei dati personali nel diritto privato euro- peo. In: CUFFARO, Vicenzo; RICCIUTO, Vicenzo. La disciplina Del trattamento dei dati personali. Giappechelli, 1997.

MAYER-SCÖNBERGER. General development of data protection in Europe. In: AGRE, Phillip; ROTENBERG, Marc (Org.). Technology and privacy: The new landscape. Cambridge: MIT Press, 1997.

MILLER, Arthur. Assault on privacy. Ann Arbor: University of Michigan, 1971.
PERLINGIERI, Pietro. L' informazione come bene giuridico. In: Rassegna di diritto civile. 2/90, p. 329.

PINÃR MAÑAS, José Luis. El derecho fundamental a la protección de dados personales (LOPD). In: (Dir.). Protección de datos de carácter personal en Iberoamérica. Valencia: Tirant Lo Blanch, 2005.

PUCCINELLI, Oscar. El habeas data em Indoiberoamérica. Bogotá: Temis, 1999.

RODOTÀ, Stefano. Elaboratori elettronici e controllo sociale. Bologna: Il Muli- no, 1973.. Repentino di fine secolo. Bari: Laterza, 1999.

SAMPAIO, José Adércio Leite Sampaio. Direito à intimidade e à vida privada. Belo Horizonte: Del Rey, 1997.

SIMITIS, Spiros. Il contesto giuridico e político della tutela della privacy. Rivista Critica Del Diritto Privato, 1997.

WACKS, Raymond. Personal information. Oxford: Clarendon Press, 1989.

WUERMELING, Ulrich. Harmonization of European Union Privacy Law. In: 14 John Marshall Journal of Computer & Information Law 411, 1996.

11. REFLEXÕES INICIAIS SOBRE A NOVA LEI GERAL DE PROTEÇÃO DE DADOS[1]

https://doi.org/10.36592/9786554600798-11

Laura Schertel Mendes

Danilo Doneda

RESUMO

O presente artigo visa analisar a importância da LGPD para a garantia dos direitos dos consumidores no século XXI e de que forma a sanção da Lei veio consolidar um marco normativo para a sociedade da informação, complementando e dialogando com outras normas do ordenamento jurídico brasileiro. Analisa os principais eixos da Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018), com especial ênfase aos princípios e direitos nela compreendidos. Por fim, examina os principais desafios para a implementação da LGPD no país.
Palavras-chave: Lei Geral de Proteção de Dados, proteção de dados, privacidade

1. Introdução

A Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), sancionada no dia 14 de agosto de 2018, inaugura no Brasil um regime geral de proteção de dados pessoais. A referida Lei vem complementar o marco regulatório brasileiro da Sociedade da Informação ao compor, juntamente com a Lei de Acesso à Informação, o Marco Civil da Internet e o Código de Defesa do Consumidor, o conjunto normativo que moderniza o tratamento da informação no Brasil. Seu objetivo é proporcionar garantias aos direitos do cidadão, ao mesmo tempo em que fornece as bases para o desenvolvimento da economia da informação, baseada nos vetores da confiança, segurança e valor.

Ao refletir sobre as principais influências que moldaram a LGPD, é possível verificar que ela se inspira, em primeiro lugar, no conceito que ficou conhecido como o modelo europeu de proteção de dados[2], amparado na Convenção do Conselho da

---

[1] Artigo originalmente publicado na Revista de Direito do Consumidor, São Paulo, v. 120, ano 27, p. 471, nov.-dez. 2018.

[2] Para uma análise sobre as características do modelo europeu de proteção de dados, cf: DONEDA, Danilo. Da Privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006; MENDES, Laura

Europa n. 108 de 1981, na Diretiva 46/95/CE e no Regulamento Geral de Proteção de Dados (Regulamento 2016/679). Isso pode ser percebido na exigência de uma base legal para o tratamento de dados, nos princípios gerais, nas regras especiais para os dados sensíveis, bem como no fato de ter como um de seus pilares a criação de uma autoridade para a aplicação da Lei.[3] São influências europeias também a edição de regras distintas de responsabilidade para o operador e controlador e a novidade da portabilidade dos dados, claramente inspirada no Regulamento Europeu.[4] Do direito americano, pode-se citar, por exemplo, a regra da notificação em caso de incidentes de segurança (art. 48, Lei 13.709/2018), expressa nas leis estaduais dos EUA de *data breach*.[5]

Além disso, também se nota clara influência da legislação brasileira também nas normas da LGPD. Do Marco Civil da Internet, por exemplo, tem-se o art. 2º, que enumera os fundamentos da proteção de dados no Brasil. Da Lei do Cadastro positivo, tem-se a regra relativa à revisão das decisões automatizadas (art. 5º, VI da Lei 12.414/2011), conceito desenvolvido anteriormente pela Diretiva européia 46/95, mas que foi introduzido na lei do cadastro positivo como um direito à revisão. Do CDC, tem-se o art. 64 da LGPD relativo ao diálogo das fontes, inspirado no art. 7º do CDC, bem como algumas regras de responsabilidade, em especial a inversão do ônus da prova, as excludentes de responsabilidade, a possibilidade de danos coletivos, assim como o conceito de tratamento impróprio de dados (art. 42, § 2º e 3º, 43 e 44, da Lei 13.709/2018).[6] Como se vê, são múltiplas as influências da LGPD: mesmo amparada no modelo europeu de proteção de dados, a LGPD dialoga com a legislação e cultura jurídica brasileira, tendo as suas normas obtido influências de inúmeras leis do nosso ordenamento.

Schertel. Privacidade, proteção de dados e defesa do consumidor. Linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

[3] European Union Agency for Fundamental Rights and Council of Europe – European Court of Human Rights, *Handbook on European Data Protection Law,* 2014, p. 187 e ss; disponível em: www.fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf.

[4] Idem, p. 228.

[5] Cf: http://www.ncsl.org/research/telecommunications-and-information-technology/2018-security-breach-legislation.aspx

[6] Para uma análise das normas setoriais que compunham no Brasil uma "colcha de retalhos" de normas sobre proteção de dados antes do advento da LGPD, ver: DONEDA, Danilo. and MENDES, Laura Schertel., 'Data Protection in Brazil: New Developments and Current Challenges', in S. Gurwirth, R. Leenes and P. De Hert. (eds). Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges, Springer, 2014.

Nesse sentido, a Lei brasileira é também a expressão da convergência internacional em torno de princípios básicos de proteção de dados no mundo, conceito esse que ficou conhecido a partir da tese de Colin Bennett.[7] O autor cunhou de convergência esse fenômeno internacional informalmente coordenado pelo qual as legislações nacionais foram se aproximando em termos de conteúdo e forma, para além das particularidades nacionais. Bennet define a convergência como a possibilidade de se identificar, na dinâmica da evolução normativa, um padrão em relação aos princípios de proteção de dados.[8]

2. Eixos principais da LGPD

É possível identificar cinco eixos principais da LGPD em torno dos quais a proteção do titular de dados se articula : i) unidade e generalidade da aplicação da Lei; ii) legitimação para o tratamento de dados (hipóteses autorizativas); iii) princípios e direitos do titular; iii) obrigações dos agentes de tratamento de dados; v) responsabilização dos agentes.

O primeiro eixo diz respeito ao âmbito de aplicação material da lei, caracterizado pela generalidade e unidade: a lei concentra-se na proteção dos dados do cidadão, independente de quem realiza o seu tratamento, aplicando-se, assim, tanto aos setores privado e público, sem distinção da modalidade de tratamento de dados (art. 3º). O seu âmbito de aplicação abrange também o tratamento de dados realizado na Internet, seja por sua concepção de lei geral, seja por disposição expressa de seu art. 1º. Estas são características fundamentais em uma lei geral, que permitem a segurança do cidadão quanto aos seus direitos independente da modalidade de tratamento de dados e quem o realize, bem como proporciona isonomia entre os diversos entes que tratam dados, o que facilita o seu fluxo e

---

[7] BENNETT, COLIN. *Regulating Privacy: data protection and public policy in Europe and the United States*. Op. Cit., p. 95 a 115. A análise comparativa realizada por Bennett envolve os seguintes países: Estados Unidos, Alemanha, Grã-Bretanha e Suécia.

[8] Segundo Bennett: "Convergência significa mais que similaridade. Denota um padrão que ultrapassa o tempo, um processo dinâmico, ao invés de uma condição estática. (...) Deste modo, a partir de uma posição em que os Estados não tinham nenhuma ou muito pouca legislação de proteção de dados e, por isso, havia diversos tipos de estratégia para o tema, um consenso emergiu durante a década de 1970, em volta de princípios. Podemos concluir, portanto, que a convergência ocorreu." Idem, p. 111 e 112.

utilização legítimos. Destaca-se que apenas os dados referentes a pessoas naturais merecem proteção no âmbito da LGPD, conforme dispõem os seus arts. 1º e 5º, I. As poucas exceções à aplicação da lei são localizadas e justificadas de forma particular, seja pela sua fundamentação em um direito fundamental (liberdade de informação, como no caso da exceção à atividade jornalística) ou interesse público relevante (como nas exceções à segurança pública e defesa nacional), nos termos do art. 4º da LGPD. Tais exceções, no entanto, são moldadas de forma a não comprometer a integridade da lei, sendo que para diversas delas refere-se à existência de legislação específica sobre proteção de dados que compreenda os princípios da LGPD.

Um dos pressupostos fundamentais da lei é que o tratamento de dados não poderá ser realizado sem que haja uma base normativa que o autorize. Assim, os tratamentos de dados pessoais deverão passar por um crivo quanto à sua legitimidade, dado que somente serão legítimos aqueles tratamentos que se enquadrem em ao menos uma das hipóteses previstas no Art. 7º ou no art. 23 da LGPD, totalizando 11 hipóteses autorizativas para o tratamento de dados pessoais. Dentre as hipóteses temos mecanismos autorizativos como o próprio consentimento do titular ou a previsão legal ou regulamentar do tratamento, acrescentando, no entanto, um conjunto de outras hipóteses que perfazem um sistema coeso. Tem se aqui o segundo eixo da LGPD.

Os requisitos para que um consentimento seja considerado válido pela lei estão previstos já na sua definição (art. 5º, XII), segundo o qual o consentimento deve ser livre, informado, inequívoco e com uma finalidade determinada.[9] Em caso de tratamento de dados sensíveis, o consentimento deve ser ainda fornecido ainda de forma específica e destacada, nos termos do art. 11, I, da LGPD. Caso o consentimento seja formulado de forma genérica ou a partir de informações enganosas prestadas ao titular, o consentimento será nulo, conforme determinam respectivamente os arts. 8º, §4º e 9º, §1º da Lei.[10]

[9] Para uma análise detalhada sobre o consentimento na proteção de dados, cf: DONEDA, Danilo. Da Privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. Ver também: Article 29 Working Party, Guidelines on consent under Regulation 2016/679. Adopted on 28 November 2017 As last Revised and Adopted on 10 April 2018. (http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051)

[10] Sobre as possíveis limitações do consentimento, cf: BIONI, Bruno Ricardo; LIMA, Cíntia Rosa Pereira de (orientadora). **Autodeterminação informacional: paradigmas inconclusos entre a tutela dos direitos**

Ainda que seja o instrumento no qual a expressão da vontade do titular dos dados classicamente encontre sua expressão, há diversas outras hipóteses de tratamento de dados capazes de, igualmente, legitimar o seu tratamento. Dentre estas, destaca-se o tratamento que visa o cumprimento de obrigação prevista em lei ou regulamento (Art 7º, II) ou para a execução de contrato do qual o titular é parte, a seu pedido (Art. 7º, V), e pela administração pública, seja quando o tratamento for necessário para a execução de política pública (Art. 7º, III) seja no exercício geral de suas competências ou cumprimento de suas atribuições legais (Art. 23).

A previsão da hipótese de tratamento para a realização de interesses legítimos do controlador ou de terceiro (Art. 7º, IX) se afigura como uma espécie de cláusula geral na qual opera-se um teste de proporcionalidade entre os interesses na utilização dos dados pessoais, que são do controlador ou de terceiro, e os direitos do titular. Neste caso, verifica-se se a realização de uma determinada finalidade com o tratamento de dados pessoais, à qual corresponde o interesse legítimo, possui efeitos potenciais para os direitos e liberdades fundamentais do titular. Se estes restarem concreta e potencialmente afetados, há de se concluir que o legítimo interesse não deve ser considerado como uma hipótese que autorize o tratamento.

Note-se, ainda, que a Lei reconhece como uma hipótese autônoma para o tratamento de dados "a proteção do crédito, inclusive quanto ao disposto na legislação pertinente" em seu Art. 7º, X. Aqui, acena-se diretamente à tradição já estabelecida na legislação brasileira de prever especificamente regras para a proteção de dados no setor de crédito, notadamente o Código de Defesa do Consumidor e a Lei 12.414/2011 (conhecida como lei do cadastro positivo). Considerando a natureza da atividade e da legislação pertinente, o dispositivo acena a uma leitura sistemática da LGPD juntamente com a legislação referente à proteção do crédito, cujas especificidades integram o regime que irá balizar o tratamento de dados no setor. Assim, elementos específicos como a inserção automática em cadastros de negativação (de acordo com o CDC) ou as regras previstas nos cadastros de adimplemento na Lei do Cadastro Positivo, específicas para o setor de crédito, continuarão a ser aplicadas e serão complementadas pelo conjunto de

da personalidade, a regulação dos bancos de dados eletrônicos e a arquitetura da internet. 2016.Universidade de São Paulo, São Paulo, 2016.

princípios e direitos da LGPD, fortalecendo a unidade sistêmica e ampliando as garantias do titular dos dados nestas situações para além das previsões setoriais.

O terceiro eixo da LGPD é composto pelos princípios e direitos do titular. O estabelecimento de uma série de princípios de proteção de dados e de direitos do titular dos dados pela Lei procura garantir, por um lado, um arcabouço de instrumentos que proporcionem ao cidadão meios para o efetivo controle do uso de seus dados por terceiros. Por outro, confere unidade sistêmica à própria disciplina da proteção de dados pessoais - que, seja pelas suas características intrínsecas ou então pelo fato de se inserir em uma tradição já amadurecida em diversos outros países, se insere em nosso ordenamento com características próprias, que se deixam entrever talvez com maior relevância justamente ao se atentar para a particularidade dos princípios e direitos próprios à matéria.

Em primeiro lugar, chama a atenção a preocupação do legislador em providenciar a enunciação de uma série de princípios na letra da lei. Este recurso leva em consideração, entre outros fatores, a novidade da matéria e a necessidade de estabelecer as principais balizas para os seus princípios fundamentais, tanto por uma questão de uniformidade e, até mesmo, didática, quanto ao se considerar a fortíssima carga substancial de diversos princípios apresentados na lei - tome-se, por todos, o exemplo do princípio da finalidade, que vincula o tratamento de dados pessoais à finalidade que motivou e justificou a sua coleta. A aplicação deste poderoso princípio tem como consequência a concretização de algumas das finalidades últimas da lei, qual seja a consideração de que o tratamento de dados pessoais são indissociáveis de uma determinada função que sempre poderá ser avaliada, ou mesmo que dados pessoais, for estarem de certa forma "afetados" por uma finalidade, jamais poderão ser considerados como mera *res in commercium*.

Ainda estão presentes uma série de outros princípios que são comuns à enorme maioria das legislações de proteção de dados hoje existentes e que defluem em geral de um tronco comum, com origem nos Fair Information Practice Principles (FIPPs)[11] e presentes em documentos como a Convenção 108 do Conselho da Europa. Estes são princípios como o do livre acesso, segurança, transparência e

[11] U.S. Department of Health, Education and Welfare. *Records, Computers and the Rights of Citizens*, 1973. Disponível em https://aspe.hhs.gov/report/records-computers-and-rights-citizens

qualidade. A Lei procura ainda abordar aspectos contemporâneos da proteção de dados e estabelecer uma série de princípios que reflitam novas demandas, como ao estabelecer o princípio da não-discriminação pelo tratamento de dados, abordando o potencial discriminatório do uso de dados ou de mecanismos de decisão automatizada que se utilizam de dados pessoais, ou mesmo o princípio da prevenção - que, no caso, se apresenta vocacionado a ser a base para o desenvolvimento de medidas relacionadas à privacidade na concepção (*Privacy by Design, PbD).*

Atente-se, ainda, para o fato de que além dos princípios literalmente enunciados no art. 6º (em número de dez) e de outros que possam ser deduzidos do texto, o *caput* do referido artigo faz referência expressa, como a um *primus inter pares*, ao princípio da boa-fé. Em tema de proteção de dados pessoais, o radicamento da boa-fé como dever de conduta é de fundamental importância, principalmente ao se levar em conta o caráter massificado de diversos mecanismos de tratamento de dados e da própria opacidade intrínseca a estas operações. Portanto, relevante o posicionamento deste princípio na LGPD, a orientar de forma ampla as relações entre titulares e agentes de tratamento seja em situações onde deveres como a transparência já estejam minimamente delineados como nas tantas outras ocasiões nas quais for necessária a qualificação de deveres de conduta.

O quarto eixo da Lei estabelece obrigações para os agentes de tratamento, estabelecendo não somente limites ao tratamento de dados em si, como também prevendo uma série de procedimentos que procuram proporcionar maior segurança e reforçar as garantias dos titulares dos dados. A natureza de diversas destas obrigações dá conta de que a LGPD vai além de proporcionar instrumentos para a defesa e proteção do titular - em outras palavras, seus efeitos não se fazem sentir somente sob requerimento do titular. Ao contrário, há uma série de mecanismos que procuram reforçar a segurança e prevenir problemas e danos no tratamento de dados. Ao mesmo tempo, há também a preocupação em estabelecer uma sistemática própria para medidas de natureza reparativa, em caso de dano.

Dentre as principais obrigações, está a do controlador instituir um encarregado pelo tratamento de dados, nos termos do art. 41 da LGPD. Note-se que se trata de uma obrigação a ser cumprida pelo controlador e não pelo operador. O encarregado terá como funções receber reclamações dos titulares, comunicar-se

com a autoridade nacional e orientar os funcionários para a que a organização cumpra com as normas de proteção de dados. A própria Lei estabelece a possibilidade de dispensa dessa obrigação, que dependerá, contudo, de norma a ser editada pela Autoridade Nacional de Proteção de Dados (art. 41, §3º).

A LGPD estabelece também uma obrigação central aos agentes de tratamento de adoção das medidas de segurança, técnicas e administrativas adequadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. É o que estabelece o seu art. 46, que inaugura o capítulo de segurança da informação da LGPD, aplicável tanto aos controladores quanto ao operadores.

O capítulo de segurança da informação é um pilar fundamental da Lei e traz pelo menos três inovações importantes para o ordenamento jurídico brasileiro quanto às obrigações dos agentes de tratamento.[12] Primeiramente, ela exige a adoção por todos que tratam dados de medidas que garantam a integridade, a confidencialidade e disponibilidade dos dados sob tratamento. Em segundo lugar, em caso de incidente de segurança, como o vazamento de dados, surge a obrigação para o controlador de comunicar a autoridade de proteção de dados, que pode determinar, conforme o caso, a adoção de medidas para mitigar os efeitos do incidente ou a ampla divulgação para a sociedade (art. 48). Em terceiro lugar, há no referido capítulo uma obrigação que se enquadra no conceito de privacy by design, conforme se extrai do art. 46, § 2º: "As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução".

Uma obrigação bastante característica é a do controlador realizar um relatório de impacto à privacidade, que é uma descrição de uma operação de tratamento de dados pessoais que execute juntamente com as medidas que tenha adotado para aumentar a segurança e mitigar o risco presente no tratamento. Este relatório será

---

[12] Para a relação entre proteção de dados e defesa do consumidor, cf: MENDES, Laura Schertel. Segurança da informação, proteção de dados pessoais e confiança. Revista de Direito do Consumidor, São Paulo, ano 22, v. 90, p. 245-261, nov.-dez. 2013.

solicitado pela Autoridade Nacional de Proteção de Dados, nos termos do art. 38 da LGPD.

O quinto eixo da Lei é o da responsabilidade dos agentes na hipótese de ocorrência de danos decorrentes do tratamento de dados e está regulado na seção III do Capítulo IV.

A consideração da responsabilidade dos agentes leva em conta, em primeiro lugar, a natureza da atividade de tratamento de dados, que a LGPD procura restringir às hipóteses com fundamento legal (Art. 7º) e que não compreendam mais dados do que o estritamente necessário (princípio da finalidade, Art. 6º, III) nem sejam inadequadas ou desproporcionais em relação à sua finalidade (Art. 6º, II).

Estas limitações ao tratamento de dados, conjuntamente com a verificação de que a LGPD assume como regra a eliminação dos dados quando seu tratamento esteja encerrado (Art. 16) e igualmente o aceno que faz em diversas oportunidades à necessidade de se levar em conta o risco presente no tratamento de dados indicam que a lei procura minimizar as hipóteses de tratamento àquelas que sejam, em um sentido geral, úteis e necessárias, e que mesmo estas possam ser limitadas quando da verificação de risco aos direitos e liberdades do titular de dados. Trata-se, desta forma, de uma regulação que tem como um de seus fundamentos principais a diminuição do risco, levando-se em conta que o tratamento de dados apresenta risco intrínseco aos seus titulares.

Assim justifica-se a opção do legislador ao optar por um regime de responsabilidade objetiva no art. 42, vinculando a obrigação de reparação do dano ao exercício de atividade de tratamento de dados pessoais.

O regime prevê ainda especificações quanto à responsabilidade de determinados agentes. No caso, o operador somente será responsabilizado por atos que cometa que sejam contrários à lei ou às instruções que lhe sejam fornecidas pelo controlador, casos nos quais aplica-se o regime de responsabilidade solidária entre controlador e operador. Ao controlador, portanto, cabe a responsabilidade nas demais hipóteses. Eventualmente, em caso de haver mais de um controlador ("controladores conjuntos"), ambos respondem solidariamente perante o titular a fim de assegurar a indenização (Art. 42, § 1º, II). São estas, aliás as duas únicas

hipóteses de solidariedade previstas na LGPD, que não tem a solidariedade como regra. A lei ainda prevê o direito de regresso em seu Art. 42, § 1º, IV.

Finalmente, a Lei prevê excludentes de responsabilidade em seu art. 43, quais sejam, quando os agentes provarem que não realizaram o tratamento de dados pessoais que lhes é atribuído (I), que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados (II) ou que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro (III)

3. Desafios atuais e possíveis soluções

No ato de sanção da LGPD, os artigos 55 a 59, que tratavam da criação de uma Autoridade Nacional de Proteção de Dados e de um Conselho de Proteção de Dados, foram vetados. Segundo as razões do veto, os referidos dispositivos incorreram em vício de iniciativa, violando o art. 61, §1, II, e cumulado com o art. 37 da Constituição.

Não há dúvidas de que a criação da Autoridade Nacional de Proteção de Dados era um pilar fundamental da LGPD. Afinal, a Lei lhe atribuía funções tão relevantes, como a de fiscalizar o tratamento de dados e sancionar o descumprimento à legislação, regulamentar hipóteses não especificadas na legislação, orientar a sociedade sobre a aplicação da lei e receber demandas sobre violações às normas de proteção de dados.

Uma análise das mais de 40 hipóteses do texto legal em que a Autoridade é chamada para atuar demonstra que a sua competência vai desde a solicitação e análise de relatórios de impacto de privacidade, determinação de medidas para reverter efeitos de vazamentos de dados, disposição sobre padrões técnicos de segurança da informação até a autorização da transferência internacional de dados pessoais. Isso demonstra que o órgão não é um mero coadjuvante do sistema de proteção de dados: ao contrário, é o seu pilar de sustentação, sem o qual todo o arcabouço normativo e principiológico não está apto a funcionar de forma adequada.

Essa é a razão pela qual cerca de cem países no mundo contam atualmente com autoridades semelhantes, tendo sido algumas delas criadas nos primórdios das proteção de dados pessoais, na década de 1970 (como as autoridades alemã, sueca

e francesa) e a maioria entre a década de 90 e os anos 2000, concomitantemente à promulgação das respectivas leis nacionais, conforme o último censo da Conferência Internacional de Autoridades de Proteção de Dados e Privacidade (ICDPPC)[13]. Dados recentes indicam que, dos 120 países que possuem leis de proteção de dados, apenas 12 não criaram uma autoridade independente responsável por sua aplicação e, por conta disto, são conhecidos internacionalmente como parte de um pequeno "corredor da vergonha" (Graham Greenleaf, 2017).

Em face do veto à ANPD, resta claro que o um grande desafio hoje para a efetividade da Lei de Proteção de Dados é a criação de uma da autoridade responsável pela sua aplicação. Fundamental para tanto será a escolha do modelo adotado, bem como a reconstituição das suas competências legais, que constavam no art. 56 e que também foram vetadas. Sem uma autoridade central, independente e com credibilidade técnica, dificilmente será possível a aplicação consistente e harmônica da Lei em setores tão diversos como os que compõem o seu âmbito de aplicação. Somente por meio de uma autoridade nesses moldes, com competência inclusive para atuar e incentivar a cooperação institucional, é que será possível superar o risco da atomização de decisões múltiplas e conflitantes entre os diversos atores legitimados para atuar na proteção de dados pessoais, considerando o atual arranjo institucional brasileiro.

Outro importante desafio diz respeito à mudança cultural, necessária para a eficaz implementação da Lei. Afinal, a LGPD traz os princípios da necessidade e da finalidade, que indicam que os dados pessoais somente poderão ser tratados quando o tratamento for necessário para atender às necessidade do controlador de dados e se a sua utilização ocorrer no âmbito do contexto ou de forma compatível com as finalidades para as quais os dados foram coletados. Isto é, faz-se necessária uma verdadeira mudança cultural para incorporarmos a compreensão de que todo dado pessoal é merecedor de proteção jurídica, por ser um meio de representação da pessoa na sociedade.

Por fim, há o desafio de interpretação sistemática das diversas legislações referentes ao tratamento de dados pessoais no Brasil, em especial, da LGPD com

---

[13] https://icdppc.org/wp-content/uploads/2017/09/ICDPPC-Census-Report-1.pdf

outras leis que tratam de setores específicos, como o Marco Civil da Internet e a Lei do Cadastro Positivo. O desafio é particularmente importante, na medida em que as soluções clássicas de conflito de leis no tempo - seja relativa à especialidade de uma das normas, seja da derrogação da lei mais antiga - não parecem ser adequadas ao presente caso. Uma solução para esse dilema reside na aplicação do diálogo das fontes, desenvolvido por Claudia Lima Marques na esteira dos ensinamentos de Erik Jayme.[14] Conforme explicado por Cláudia Lima Marques, o diálogo das fontes é "a atual aplicação simultânea, coerente e coordenada das plúrimas fontes legislativas, leis especiais (como o CDC, a lei de seguro-saúde) e gerais (como o CC/2002), com campos de aplicação convergentes, mas não mais iguais.[15]

Conclusão

O tema da proteção de dados tornou-se um componente fundamental para a proteção do cidadão, do consumidor e para a própria segurança da Sociedade em um mundo hiper conectado, na qual os dados pessoais são o insumo de inúmeras atividades econômicas no mundo online e off-line, sendo essenciais também para a atuação pelo setor público.[16] Basta se pensar no fluxo de dados de crédito e dados financeiros para análise da capacidade de pagamento dos consumidores, dados sobre a saúde dos pacientes, sobre o comportamento e hábitos coletados na internet, entre outros, o que demonstra a ubiquidade dos meios informáticos (*ubiquitous computing*[17]), assim como do processamento de dados.

---

[14] MARQUES, Claudia Lima. "O 'diálogo das fontes' como método da nova teoria geral do direito: um tributo à Erik Jayme" In: MARQUES, Claudia Lima (coord.). *Diálogo das Fontes. Do conflito à coordenação de normas do direito brasileiro*. São Paulo: Revista dos Tribunais, 2012.

[15] BENJAMIN, Antonio Herman; MARQUES, Claudia Lima; BESSA, Leonardo, *Manual de Direito do Consumidor*. São Paulo: Revista dos Tribunais, 2008, p. 85. Os autores explicam a razão do termo diálogo: "'Diálogo' porque há influencias recíprocas, 'diálogo' porque há aplicação conjunta de duas normas ao mesmo tempo e ao mesmo caso, seja complementarmente, seja subsidiariamente, seja permitindo a opção pela fonte prevalente ou mesmo permitindo uma opção das leis em conflito abstrato – uma solução flexível e aberta, de interpenetração, ou mesmo a solução mais favorável ao mais fraco da relação (tratamento diferente dos diferentes)" - p. 87 e 88.

[16] VESTING, Thomas, "§20 Die Bedeutung von Information und Kommunikation für die verwaltungsrechtliche Systembildung", In: HOFFMANN-RIEM, Wolfgang et al, *Grundlagen des Verwaltungsrecht, Band II,* München: Beck, 2008, p. 22.

[17] MATTERN, Friedemann, "Allgegenwärtige Datenverarbeitung – Trends, Visionen, Auswirkungen...". In: ROßNAGEL, Alexander et al. *Digitale Visionen: Zur Gestaltung allgegenwärtiger Informationstechnologien,* Berlin: Springer, 2008. Cf também: HARTMANN, Maren, WIMMER, Jeffrey,

A utilização legítima e responsável dos dados pessoais proporciona ao cidadão a confiança necessária para compartilhá-los sempre que julgar cabível, bem como garante aos agentes de tratamento segurança jurídica para que possa utilizá-los de forma transparente em seus modelos de negócio. Para que se alcance tal finalidade, desenvolveu-se um sistema de normas proteção de dados, que envolve o estabelecimento de uma série de procedimentos, princípios e direitos, que limitam o processamento de dados pessoais ao mesmo tempo que empoderam o cidadão para controlar o fluxo de seus dados. Nesse sentido, a sanção da LGPD foi, certamente, um enorme avanço no marco normativo brasileiro.

Ocorre, no entanto, que a sua efetiva implementação depende da constituição de uma autoridade de proteção de dados pessoais, amparada em um tripé consistente em poder sancionatório, expertise e independência. Sem a construção dessa arquitetura regulatória, não será possível alcançar o seu principal objetivo, que é o de consolidar a confiança da sociedade da na infraestrutura de informação e comunicação, garantindo direitos, ampliando a inovação e propiciando maior competitividade entre serviços que utilizam de forma legítima e transparente os dados pessoais. A efetiva aplicação da LGPD dependerá também de uma mudança cultural que compreenda que todo dado pessoal é merecedor de proteção jurídica. Ainda, é fundamental consolidar-se uma interpretação sistemática da LGPD com os demais diplomas normativos que dispõem sobre tratamento de dados pessoais, no moldes do diálogo das fontes, possibilitando a aplicação simultânea dos princípios e regras gerais da LGPD com as regras setoriais.[18]

Por fim, deve-se ressaltar que a disciplina de proteção de dados pessoais diz respeito a uma matéria em constante evolução e que o ordenamento jurídico brasileiro deve ficar atento para os desenvolvimentos tecnológicos que cotidianamente alteram a vida dos cidadãos, as formas de trabalho, as nossas cidades e a economia na sociedade contemporânea. Tais transformações acabam

---

Einleitung. In: HARTMANN, Maren, WIMMER, Jeffrey, *Digitale Medientechnologien: Vergangenheit – Gegenwart – Zukunft.* Wiesbaden: VS, 2011, p. 21.

[18] Como bem lembram Alexandre Veronose e Noemy Melo, tal diálogo terá que ser feito também entre as normas que regulam as atividades do setor de telecomunicações, de comunicação social e das tecnologias da informação. (VERONESE, Alexandre; MELO, Noemy. O Projeto de Lei 5.276/2016 em contraste com o novo Regulamento Europeu (2016/679 UE). Revista de Direito Civil Contemporâneo. vol. 14. ano 5. p. 71-99. São Paulo: Ed. RT, jan.-mar. 2018)

por influenciar também o desenvolvimento da temática de proteção de dados. Importante evidência dos novos desenvolvimentos nessa seara foi a revisão pela OCDE das Diretrizes relativas à proteção de dados pessoais e ao fluxo de dados transfronteiriços de 2013[19], a edição do Regulamento europeu de proteção de dados em 2016, que entrou em vigor em 25 de maio de 2018, assim como a recém aprovada Lei de proteção de dados da Califórnia[20]. Para além dessas modificações no âmbito institucional, a transformação do conceito da privacidade e proteção de dados pode ser vista também na teoria da informação, como demonstra a obra de Helen Nissenbaum. A autora defende um conceito de privacidade mais complexo e amplo do que as definições até então conhecidas, cujo foco era o controle do indivíduo sobre as suas informações pessoais ou a preservação de eventos íntimos e privados.[21]

Do exposto, percebe-se que LGPD foi um importante passo rumo ao fortalecimento do marco normativo da sociedade da informação no Brasil. É preciso agora desenvolver uma cultura de proteção de dados, construir uma sólida estrutura institucional para a aplicação da LGPD, assim como uma doutrina aprofundada sobre os diferentes temas tratados pela lei, propiciando segurança jurídica para os atores da economia digital, a proteção da confiança do titular dos dados e incentivando o desenvolvimento econômico do país nessa área[22].

---

[19] Essas Diretrizes, que constituíram o primeiro acordo internacional sobre o tema, haviam sido editadas em 1980, foram revisadas pela primeira vez em 2013. Disponpivel em: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[20] https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180AB375

[21] Nissenbaum define privacidade como "integridade contextual" (contextual integrity), afirmando que a privacidade não é um direito ao sigilo, nem um direito de controle, mas sim o fluxo apropriado de informação pessoal, conforme normas informacionais orientadas pelos contextos sociais (context-relative informational norms). A violação da privacidade dar-se-á então sempre que essas normas informacionais forem desobedecidas. A verificação da violação da privacidade sob essa perspectiva requer a análise de uma série de critérios, tais como contextos (ambientes sociais estruturados), atores (emissores, receptores e sujeitos da informação), atributos (tipos de informação) e princípios de transmissão (confidencialidade, reciprocidade, necessidade, etc). Além disso, ela afirma que em determinados casos faz-se necessária uma avaliação mais ampla sobre os riscos causados pelo fluxo de informações à autonomia e à liberdade do indivíduo, assim como à igualdade, à justiça e à democracia. (NISSENBAUM, Helen. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford: Stanford Law Books, 2010.)

[22] Ver estudo sobre a importância da confiança digital para as organizações: https://www.ca.com/us/collateral/white-papers/the-global-state-of-online-digital-trust.html

Bibliografia

BENJAMIN, Antonio Herman; MARQUES, Claudia Lima; BESSA, Leonardo, *Manual de Direito do Consumidor.* São Paulo: Revista dos Tribunais, 2008.

European Union Agency for Fundamental Rights and Council of Europe – European Court of Human Rights, *Handbook on European Data Protection Law,* 2014, available at: www.fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf.

BIONI, Bruno Ricardo; LIMA, Cíntia Rosa Pereira de (orientadora). Autodeterminação informacional: paradigmas inconclusos entre a tutela dos direitos da personalidade, a regulação dos bancos de dados eletrônicos e a arquitetura da internet. 2016.Universidade de São Paulo, São Paulo, 2016.

DONEDA, Danilo. Da Privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo e MENDES, Laura Schertel., 'Data Protection in Brazil: New Developments and Current Challenges', in S. Gurwirth, R. Leenes and P. De Hert. (org). Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges, Springer, 2014.

HARTMANN, Maren, WIMMER, Jeffrey, Einleitung. In: HARTMANN, Maren, WIMMER, Jeffrey, *Digitale Medientechnologien: Vergangenheit – Gegenwart – Zukunft.* Wiesbaden: VS, 2011.

MENDES, Laura Schertel. Segurança da informação, proteção de dados pessoais e confiança. Revista de Direito do Consumidor, São Paulo, ano 22, v. 90, p. 245-261, nov.-dez. 2013.

MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor. Linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MENDES, Laura Schertel. Segurança da informação, proteção de dados pessoais e confiança. Revista de Direito do Consumidor, São Paulo, ano 22, v. 90, p. 245-261, nov.-dez. 2013.

MARQUES, Claudia Lima. "O 'diálogo das fontes' como método da nova teoria geral do direito: um tributo à Erik Jayme" In: MARQUES, Claudia Lima (coord.). *Diálogo das Fontes. Do conflito à coordenação de normas do direito brasileiro*. São Paulo: Revista dos Tribunais, 2012.

MATTERN, Friedemann, “Allgegenwärtige Datenverarbeitung – Trends, Visionen, Auswirkungen...“. In: ROßNAGEL, Alexander et al. *Digitale Visionen: Zur Gestaltung allgegenwärtiger Informationstechnologien,* Berlin: Springer, 2008.
NISSENBAUM, Helen. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford: Stanford Law Books, 2010.

U.S. Department of Health, Education and Welfare. *Records, Computers and the Rights of Citizens*, 1973. Disponível em https://aspe.hhs.gov/report/records-computers-and-rights-citizens

VERONESE, Alexandre; MELO, Noemy. O Projeto de Lei 5.276/2016 em contraste com o novo Regulamento Europeu (2016/679 UE). Revista de Direito Civil Contemporâneo. vol. 14. ano 5. p. 71-99. São Paulo: Ed. RT, jan.-mar. 2018.

VESTING, Thomas, “§20 Die Bedeutung von Information und Kommunikation für die verwaltungsrechtliche Systembildung“, In: HOFFMANN-RIEM, Wolfgang et al, *Grundlagen des Verwaltungsrecht, Band II,* München: Beck, 2008.

12. REGISTRO DA SUSTENTAÇÃO ORAL DO DANILO DONEDA NO JULGAMENTO DA ADI Nº 6389

https://doi.org/10.36592/9786554600798-12

Danilo Doneda

Caros Colegas,

Venho aqui, em nome do PARTIDO SOCIALISTA BRASILEIRO, na Ação Direta de Inconstitucionalidade 6.389, apresentar as razões pelas quais requeremos a declaração de inconstitucionalidade dos artigos 2º, caput e §1º e 3º da Medida Provisória 954, de 17 de abril de 2020.

Trata-se de Medida Provisória que obriga a disponibilização de dados pessoais dos usuários de operadoras de telefonia fixa e móvel com o Instituto Brasileiro de Geografia e Estatística (IBGE).

O presente caso diz respeito, na verdade, não somente a pesquisas realizadas pelo IBGE, porém sobre os próprios parâmetros constitucionais da proteção de dados no Brasil e, ao final, ao valor e significado dos dados pessoais dos brasileiros para a nossa liberdade, personalidade e democracia.

A MP 954 estabelece a obrigação legal de disponibilização ao IBGE de um volume de dados pessoais de mais de 140 milhões de brasileiros, sem estabelecer, contudo, as garantias necessárias para a proteção dos dados dos cidadãos, isto em pleno século XXI, quando se sabe que o acesso indevido ou incidentes de segurança são corriqueiros e estampam cotidianamente as capas de jornais.

Trata-se da disponibilização de um banco de dados estruturado, que facilita a localização e associação de pessoas com seus telefones e endereços - dados que, até um passado relativamente recente, estavam presentes em listas telefônicas impressas. As listas telefônicas, em uma sociedade que ainda não era digital, eram um dos poucos meios para uma pessoa ou empresa se fazer notar e seus espaços chegavam a ser muito disputados. A presença do número do telefone na lista dependia da vontade dos particulares.

Os tempos mudaram, e muito! A disponibilização de um número telefônico tem, hoje, efeitos completamente diferentes e aumenta drasticamente a vulnerabilidade dos cidadãos. Antes, por exemplo, sequer seria possível telefonar para todos os números em uma lista sem despender esforços tremendos, com um custo altíssimo; ao passo que hoje, a possibilidade técnica de atingir dezenas de milhões de pessoas por meio de aplicativos e redes sociais a custo infinitamente menor é real, desde que se esteja de posse dos números telefônicos celulares.

Hoje, o número de celular é muito mais do que um identificador. Ele acaba sendo o login, a forma de acesso do cidadão a um grande número de serviços, e a sua disponibilização pode afetar a forma dele se relacionar com estes serviços. Além disto, a tecnologia hoje disponível torna possível abordar individualmente pessoas segundo as suas características, mesmo a partir de um conjunto imenso de dados. Esta abordagem individualizada, aliás, foi o elemento principal do escândalo envolvendo a empresa *Cambridge Analytica*. Como já foi dito, na Era da Informação, o palheiro muitas vezes não é mais capaz de esconder a agulha, - metáfora para a informação volumosa e desordenada que existe sobre nós. Afinal, o tratamento abusivo de dados pessoais pode vulnerabilizar sobremaneira a pessoa, proporcionando-lhe riscos potenciais muito maiores e diversos do que aqueles atinentes à sua privacidade, como a vigilância, a discriminação e até mesmo prejuízos econômicos. Como bem expresso na decisão da Anatel, ao analisar o tratamento de dados previsto na MP:

> (...) não se está a falar de informações insignificantes, mas dachave de acesso individual a milhões de pessoas, com um alto valornão só para políticas públicas, mas também para práticas comerciais que – em determinadas vertentes – causam inclusive distúrbios na vida diária. Portanto, repousa sobre os detentores desses dados um dever claro que eles sejam usados somente da forma pretendida, assegurada a redução de riscos de seus vazamentos ou manipulação por terceiros[1].

[1] ANATEL. Voto Nº 30/2020/PR. Processo nº 53500.017367/2020-40.

O IBGE realiza atividade imprescindível para a devida execução de políticas públicas. A atividade estatística, para cumprir sua função primordial, deve estar fortemente alicerçada na confiança que as instituições estatísticas incutem na sociedade. Para que esta confiança se concretize, a atividade estatística depende fundamentalmente da aplicação efetiva do segredo estatístico, ao garantir que a disponibilização de informações completas e acuradas não seja dificultado ou impossibilitado por suspeitasde que estas poderiam ser utilizadas em detrimento do cidadão.

A atividade estatística, para cumprir sua função primordial, deve estar fortemente alicerçada na confiança que as instituições estatísticas incutem na sociedade, confiança que depende fundamentalmente da aplicação efetiva do segredo estatístico, ao garantir que a disponibilização de informações completas e acuradas não seja dificultado ou impossibilitado por suspeitas de que estas poderiam ser utilizadas em detrimento do cidadão.

O uso de informações para fins exclusivamente estatísticos é uma tônica nos estados democráticos e qualquer réstia de desconfiança sobre sua integridade prejudica a execução de políticas públicas e, consequentemente, prejudica toda a coletividade.

Tomemos um caso, de memória recente, para ilustrar a importância do segredo estatístico: a Suspensão de Liminar (Sl) 1103, na qual o IBGE recorreu contra decisão que o obrigara a fornecer ao MPF os dados necessários à identificação de 45 crianças domiciliadas em Bauru (SP), que, segundo o Censo de 2010, não foram regularmente registradas nos cartórios de registro civil da cidade. Em decisão monocrática, suspendendo a liminar, a Ministra Carmen Lúcia ressalvou que:

> o afastamento do sigilo estatístico imposto pela decisão contrastada dispõe de potencialidade lesiva à ordem pública, porabalar a confiança daqueles que prestam as informações aos entrevistadores do IBGE, comprometendo a fidelidade e veracidade dos dados fornecidos e, por conseguinte, a própria finalidade daqueleInstituto, a subsidiar a elaboração de políticas públicas em benefício da sociedade.

A continuidade desta tradição e a garantia de que o IBGE continue exercendo seu papel fundamental para o desenvolvimento dependem, hoje, cada vez mais de fatores que vãoalém do segredo estatístico, incluindo considerar em toda a sua amplitude o direito à prteção de dados pessoais.

O direito à proteção de dados pessoais surge para colocar o cidadão no controle sobre seus próprios dados e reduzir riscos envolvidos no seu tratamento, reconhecendo, ao mesmo tempo, que há diversos tratamentos legítimos que devem ser tornados transparentes e claros para os cidadãos.

Uma decisão de 1983 do Tribunal Constitucional alemão foi decisiva para o desenvolvimento deste direito, ao reconhecer uma garantia constitucional específica relacionada à proteção de dados pessoais. Significativamente, tratava-se também de umcaso referente à atividade estatística: era contestada uma lei federal que regia o censo alemão de 1982.

Ao analisar o caso, o Tribunal reconheceu que avanços tecnológicos tornavam possível oprocessamento de dados em proporção jamais vistas, o que demandava o que fosse revisitada a interpretação de alguns direitos fundamentais, em razão do surgimento de ameaças e riscos até então impensáveis, não somente à privacidade, porém a diversas liberdades e garantias fundamentais. Assim, a Corte reconheceu a existência de um direito à autodeterminação informacional, formulado a partir do direito geral de personalidade e voltado a garantir ao cidadão o direito de controlar a amplitude da divulgação ou utilização de qualquer aspecto relacionado a sua personalidade por meio de seus dados pessoais. Nas palavras da Corte:

> Hoje, com ajuda do processamento eletrônico de dados, informações detalhadas sobre relações pessoais ou objetivas de uma pessoa determinada ou determinável (dados relativos à pessoa [cf. § 2 I BDSG – Lei Federal sobre a Proteção de Dados Pessoais]) podem ser, do ponto de vista técnico, ilimitadamente armazenados e consultados a qualquer momento, a qualquer distância e em segundos. Além disso, podem ser combinados, sobretudo na estruturação de sistemas de informação integrados, com outros bancos de dados, formando um quadro da personalidade relativamente completo ou

> quase, sem que a pessoa atingida possa controlar suficientemente sua exatidão e seu uso.

Ao reconhecer a centralidade do controle sobre as próprias informações para a proteçãoda personalidade no contexto do tratamento automatizado de dados, o Tribunal realizounotável trabalho de atualização das garantias fundamentais em vista das circunstâncias tecnológicas da época. Este trabalho de atualização por conta da mudança de um contexto tecnológico pode ser observado em outras situações com certas similaridades.

Na jurisprudência norte-americana, o caso *Olmstead v. United States*, de 1928, tratava da aplicação da quarta emenda à Constituição norte-americana, referente ao direito contra a intromissão e buscas não autorizadas na residência, documentos e bens de uma pessoa, em um caso que envolvia a utilização de grampos telefônicos. No julgamento, teve destaque o voto do juiz Louis Brandeis, que chamou a atenção para a necessidade de atualizar a interpretação da Quarta Emenda conforme a realidade tecnológica:

> Na aplicação da Constituição, nossa preocupação não deve ser somente sobre o que foi, porém o que será. O progresso da ciência, aomunir o governo de meios automatizados de espionagem, não irá parar com a escuta telefônica. Um dia, surgirão meios para que o governo, sem ter que remover papéis de uma gaveta, possa utilizá-los em juízo, tornando possível expor os fatos mais íntimos ocorridos dentro de uma casa. O progresso científico proporcionará meios para explorar crenças, pensamentos e emoções sequer expressas. (...). Serápossível que a Constituição não nos ofereça meios de proteção contra tais invasões da segurança individual?[2].

O voto de Brandeis se constituiu em um poderoso argumento que fundamentou, posteriormente, o caso *Katz v. United States*, de 1967[3]3, a partir do qual a quarta emendapassou a ser aplicada frente a ameaças tecnológicas. Até

---

[2] Olmstead v. United States, 277 U.S. 438 (1928).
[3] Katz v. United States, 389 U.S. 347 (1967).

hoje, o voto continua sendo citado e referido em casos paradigmáticos, como o recente *Carpenter v. United States* [4], no qual foi reconhecida a proteção constitucional para o conteúdo de telefones celulares,observando que a Suprema Corte é obrigada a garantir que o progresso da ciência não viole a Constituição à medida que meios mais intrusivos de violação da privacidade se tornem disponíveis. Temos aqui uma importante inspiração: não podemos permitir quea Constituição se torne obsoleta frente ao desenvolvimento tecnológico!

Merece igualmente menção o caso do direito fundamental à garantia da confidencialidade e da integralidade dos sistemas técnico-informacionais, reconhecida pelo Tribunal Constitucional alemão em 2008 como uma espécie de desdobramento do direito fundamental à autodeterminação informativa, pelo qual a garantia à integralidade de sistemas era uma medida indireta de proteção aos direitos fundamentasde privacidade, liberdade e autodeterminação.

A atualização do direito confirme o paradigma tecnológico atual é imperativa em uma época em que do tratamento leal de nossas informações pessoais depende parcela essencial das nossas liberdades. O direito à proteção de dados pessoais procura, justamente, prover o ordenamento com instrumentos que possam vislumbrar e seantecipar a novos riscos trazidos pelas novas tecnologias, partindo do paradigma do direito à privacidade, porém ampliando-o de forma a se configurar em um estatuto da pessoa em relação ao controle de suas informações.

Resulta, portanto, fundamental atualizar a interpretação da Constituição Federal para o paradigma tecnológico da Sociedade em que vivemos. Os instrumentos para isto já se encontram presentes em nossa ordem jurídica, a partir da leitura da cláusula geral da proteção à personalidade na Constituição Federal, juntamente com a interpretação atualizada das garantias à privacidade informacional presentes no art. 5º, X-XII, da CF.

Assim, os termos da MP 954 devem ser avaliados no contexto atual e sob a ótica constitucional, considerando os riscos que se multiplicam e a necessidade de salvaguardas para além da estrita verificação do segredo estatístico.

---

[4] Carpenter v. United States, 16-402 U.S. 585 (2018)

A integralidade da base de dados dos usuários de telefonia fixa e móvel, que, nos termosda MP 954 deve ser transferida ao IBGE, representa volume de dados pessoais imensamente maior do que a amostragem necessária para a realização da PNAD - Pesquisa Nacional por Amostra de Domicílios, que gira em torno de pouco mais de 200 mil respondentes. Esta enorme desproporção representa clara violação ao princípio da proporcionalidade e do princípio da minimização, princípios clássicos de proteção de dados, e ensejam em risco desnecessário para a sociedade.

A diminuição de riscos no tratamento de dados pessoais é fator essencial do direito à proteção de dados. Um banco de dados pessoais da dimensão e importância deste coberto pela MP 954 inspira atenção pela necessidade de que se busquem alternativas para a realização da pesquisa sem que se configurem riscos maiores para os cidadãos. Naproposta feita pela MP, é patente que o próprio recurso à disponibilização deste banco de dados sem a consideração de outras alternativas viáveis implica a não observância dodever razoável de cuidado e da aplicação do princípio da precaução.

Modernas técnicas vêm sendo desenvolvidas para a obtenção de um máximo de utilidadea partir de grandes bases de dados com um mínimo de risco para os cidadãos. São técnicas de vários matizes, desde a intermediação dos dados por fiduciários ou a produção de amostragens pelo próprio gestor do banco de dados de origem por técnicasde OPAL (*Open Algorithm*) que podem tornar uma operação como a proposta pela MP segura e útil sem demandar a disponibilização integral de um banco de dados.

Outros elementos, ou melhor, a falta destes, contribuem para caracterizar o descompassoda MP 954 com as garantias constitucionais relacionadas à proteção de dados pessoais. A ausência de mecanismos de supervisão específicos, que aliás evidencia a mora em que se encontra o Poder Executivo federal no tocante à instalação da Autoridade Nacional deProteção de Dados, é elemento incremental do potencial de risco da operação. Ainda, a própria menção pela MP de um relatório de impacto à proteção de dados pessoais que, no entanto, somente será devido após a disponibilização dos dados, demonstra a ausência do dever de cautela devida,

visto que riscos referentes à disponibilização de dados, uma vez consumados, costumam ser irreversíveis.

O reconhecimento do caráter constitucional da proteção aos dados pessoais opera a superação de uma concepção, hoje anacrônica, segundo a qual seria possível realizar a governança de dados pessoais a partir de considerações sobre o direito à privacidade e osegredo ou sigilo. A consolidação deste direito garante que os dados pessoais possam serutilizados com maior facilidade e com base jurídica sólida quando necessários e para fins legítimos, garantida a transparência, segurança e os direitos individuais, diminuindo osriscos sobre as operações de tratamento.

O recurso a dados pessoais de qualidade é pressuposto para a execução de políticas públicas e deve ser não só almejado como protegido. No caso em tela, a utilização de procedimentos que diminuam o risco aos dados pessoais virá a proteger a própria atividade estatística, seja dos riscos inerentes ao processamento dos dados, seja do risco eventual desta ser vista como um repositório de informações cujo controle possa ser útilpara outras lógicas e finalidades que não a pesquisa estatística.

O jurista Stefano Rodotà, professor emérito da Universidade de Roma *La Sapienza* e quefoi por oito anos o comissário italiano para o tema, observou, certa feita que:

> A proteção de dados pessoais constitui não apenas um direito fundamental entre outros: é o mais expressivo da condição humana contemporânea. Relembrar isto a cada momento não é mera retórica,pois toda mudança que afeta a proteção de dados tem impacto sobreo grau de democracia que nós podemos experimentar[5].

Estamos em um momento de construção, em um momento de notável aceleração de processos históricos. Em um momento como este, caso o compartilhamento de dados como o ensejado pela MP 954 seja tornado possível

---

[5] RODOTÀ, Stefano. A vida na sociedade da vigilância. A privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 21.

sem a aposição de garantias efetivassobre a finalidade, transparência, segurança e proporcionalidade e seu devido controle, arrisca-se a consolidação de uma situação irreversível para a garantia dos direitos fundamentas.

A Constituição Federal, que foi pioneira ao prever institutos modernos como a ação de Habeas Data, mais do que nunca deve ser interpretada à luz dos novos desafios do séculoXXI, no sentido do reconhecimento da tutela constitucional da proteção dos dados pessoais, garantindo a privacidade, liberdade e autodeterminação do cidadão frente ao atual contexto tecnológico, concretizando elementos para que o brasileiro goze de efetiva cidadania na sociedade da informação e apontando a interpretação constitucional para os novos desafios que ainda estão por vir.

Por todo o exposto, o Partido Socialista Brasileiro requer, reconhecida a natureza constitucional do direito à proteção de dados pessoais, a ratificação da medida liminar, para que seja mantida a suspensão dos dispositivos referidos da Medida Provisória 954 e, por consequência, para que o IBGE se abstenha de obter informações pessoais juntoàs operadoras de telefonia fixa e móvel.

13. REGISTRO DA SUSTENTAÇÃO ORAL DO DANILO DONEDA NO JULGAMENTO ADI Nº 6649

https://doi.org/10.36592/9786554600798-13

Danilo Doneda

Excelentíssimo Sr. Presidente desta Corte Suprema;
Excelentíssimo Sr. Ministro Relator;
Excelentíssimos Sras. e Srs. demais integrantes desta Corte;
Eminente Sr. Vice Procurador-Geral da República;
Caras e caros Colegas;
Senhoras e Senhores,

O que está em jogo hoje é assegurarmos que a modernização da administração pública, através de uma gestão e planejamento que façam uso de informações, seja acompanhada de garantias contra os riscos ao cidadão derivados do tratamento de seus dados pessoais; o que está em jogo é garantir que os custos desta modernização não recaiam sobre o cidadão, que tem o direito de poder continuar confiando no Estado como depositário de seus dados pessoais. O que está em jogo hoje nada mais é, enfim, do que adequar a ordem jurídica aos dilemas e demandas de nosso tempo.

Venho, em nome do CONSELHO FEDERAL DA ORDEM DOS ADVOGADOS DO BRASIL, apresentar as razões pelas quais requeremos a declaração de inconstitucionalidade do Decreto n. 10.046, de 2019.

O Decreto dispõe sobre compartilhamento de dados no âmbito da administração pública federal. Ele, porém, desarma um conjunto de garantias que são necessárias para o exercício da cidadania em uma sociedade ávida pela informação, garantias estas que foram duramente conquistadas e consolidadas pelo direito fundamental à proteção de dados e pela LGPD - Lei Geral de Proteção de Dados. Assim, este compartilhamento, que é imprescindível para a eficácia dos mais modernos métodos de gestão, acaba por se converter em fator de insegurança e

ilegalidade, além de alijar o cidadão do controle e ciência sobre a utilização de seus dados pelo poder público.

Esta inconstitucionalidade se faz evidente por motivos formais e materiais. Formalmente, manifesta-se com clareza a extrapolação da competência regulamentar pelo Presidente da República: Ao procurar regulamentar as leis 12.527/2011 (LAI), 13.444/2017 (ICN) e 13.709/2018 (LGPD), opera o Decreto concreta inovação no ordenamento jurídico ao dispor sobre direitos e garantias fundamentais dos cidadãos, limitando-as concretamente, bem como aumentando os riscos a que os cidadãos estão expostos.

Este Decreto foi sancionado nos estertores de um paradigma hoje vetusto e ultrapassado. Seu texto remonta a uma época na qual dificuldades crônicas de acesso a informações para alimentar políticas públicas eram tais que dados pessoais eram muitas vezes usados de forma virtualmente irrestrita e sem garantias para os cidadãos. Este cenário, no entanto, mudou rápida e radicalmente com o desenvolvimento de tecnologias de processamento de dados, gerando a necessidade da regulação destes tratamentos justamente para contemplar a proteção do cidadão - enfim, é justamente para adequar o sistema de garantias constitucionais às novas tecnologias dominantes que surgiu uma legislação como a LGPD. Neste novo paradigma, os dados pessoais deixaram de ser um recurso escasso e juridicamente pouco relevante para ter, inclusive, um valor jurídico intrínseco - como se tornou costume mencionar, os dados pessoais se tornaram o combustível da nova economia da informação - assim como sua proteção se tornou essencial para a garantia da cidadania.

O Decreto, no entanto, como se a modernidade lhe fosse estranha ou inconveniente, parece ignorar este novo paradigma ao considerar a informação pessoal sob prisma meramente utilitarista e tecnocrático, em frontal desacordo com o que afirmou esta Excelsa Corte em julgamento paradigmático de 2020 quando da propositura por este CF-OAB e por uma série de partidos políticos de ADIs em face da MP954, que pretendia justamente o compartilhamento de dados pessoais entre dois entes públicos sem maiores salvaguardas para os cidadãos. Naquela ocasião, constatou esta Corte que não existem mais dados pessoais insignificantes: isto é, todo tratamento de dados pessoais apresenta um potencial de risco intrínseco que

demanda a implementação de mecanismos de proteção aos titulares para que possa se legitimar em uma sociedade democrática.

Com aquela decisão, a proteção de dados no Brasil passou a proporcionar a garantia dos direitos inalienáveis do cidadão na era digital, posicionando-se na nossa ordem jurídica como instrumento para a consolidação da democracia e das liberdades. Hoje, a partir de seus dados pessoais, cidadãos podem ser analisados, avaliados, monitorados, discriminados e… controlados, além de extirpados de sua autonomia e dignidade por frequentes decisões que afetam suas vidas serem tomadas a partir de seus dados, sem o devido processo e sem que tenham oportunidade de participação. É assim, aliás, que assevera a prof Laura Schertel Mendes em artigo publicado recentemente no jornal O Globo, no qual destaca como o poder informacional, que é derivado do controle sobre o uso da informação, pode ser malversado a prejuízo dos direitos e garantias fundamentais.

Materialmente, verificamos que o Decreto não estabelece o devido equilíbrio entre o compartilhamento de dados pessoais com os imperativos decorrentes do direito fundamental à proteção de dados, pelos motivos elencados em nosso pedido e que passo a resumir muito sucintamente.

Em primeiro lugar, o referido Decreto é silente quanto aos riscos potenciais aos cidadãos resultantes do compartilhamento. Esta lacuna é ressaltada pelo fato da categoria de dados sensíveis - aqueles que apresentam maior potencial discriminatório -, ser solenemente ignorada pelo Decreto que, por outro lado, não se furta a validar tratamentos de dados que são, de fato, sensíveis - por exemplo, dados biométricos, como quando se refere a "características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar" (art. 2º, II, do Decreto nº 10.046/2019).

O Decreto não esboça qualquer regime particular de proteção para estes dados.

O decreto prossegue seu rol de desacertos ao menoscabar o princípio da transparência e, ainda, em diversos momentos aumentar uma opacidade que já é intrínseca aos tratamentos de dados, como quando possibilita a interligação de

bases de dados de diferentes órgãos públicos sem a necessidade de acordos ou convênios entre estes.

Outra lacuna clamorosa do Decreto, no que talvez seja a sua falha estrutural que mais o caracteriza como uma normativa ultrapassada, é a ausência de mecanismos que proporcionem o devido controle e transparência acerca da finalidade para a qual os dados pessoais são compartilhados pela Administração Pública. A LGPD prevê uma base legal para o tratamento de dados pela Administração Pública que, no entanto, restringe-se aos dados que são necessários para as suas atividades específicas, nunca para uma cadeia genérica, indefinida e indeterminada de finalidades que podem ser inadequadas ou não relacionadas.

O tratamento de dados pelo setor público não é uma finalidade em si, ainda que o Decreto pareça pressupor que o seja. A finalidade que justifica este tratamento deve ser considerada e avaliada de acordo com as competências dos órgãos envolvidos, as políticas públicas em questão, a natureza dos dados e uma série de outros elementos. A hipertrofia da finalidade do tratamento que é operada pelo Decreto implica, na prática, na formulação de uma verdadeira nova base legal, extrapolando em muito, portanto, o poder regulamentar.

Seria natural que, do Decreto, constassem soluções úteis e inovadoras para a garantia do direito fundamental à proteção de dados - porém não é isso que ocorre, criando-se o grave risco de consolidação de práticas que fulminam os direitos fundamentais e erodem a confiança do cidadão nos agentes públicos. Ante estes riscos, um sistema de otimização da gestão de políticas públicas, como o Cadastro Base do Cidadão, por exemplo, pode facilmente se transmudar em ferramenta de vigilância e controle social, ainda mais se eventualmente cair em mãos de um governo com pouco apreço pelas liberdades democráticas - por isto, justamente, as garantias sobre dados pessoais não dizem respeito somente a interesses individuais, porém detêm função da maior importância para o Estado Democrático de Direito.

Felizmente, há diversas formas de sanar as deficiências do Decreto. Várias medidas capazes de garantir a legitimidade do compartilhamento de dados devem ser consideradas, tais como (1) a efetiva verificação de compatibilidade de finalidades nos compartilhamentos; (2) a consideração do risco inerente, com a instituição de medidas de avaliação de risco e atenção particular aos dados

sensíveis; (3) a criação de plataformas que promovam a transparência em relação ao uso dos dados pessoais e que permitam ao cidadão exercer seus direitos e realizar escolhas relevantes sobre a utilização de seus dados, dentre outras - todas estas ausentes do Decreto.

Ademais, no contexto do julgamento no qual esta Egrégia Corte havia reconhecido, em 2020, o direito fundamental à proteção de dados, foram identificados diversos parâmetros para a sua implementação, consolidando um verdadeiro arcabouço para balizar o compartilhamento de dados pessoais. Estes elementos englobam, além dos que já mencionamos, a necessidade da (1) construção de um sistema de governança dos dados pessoais acessível ao cidadão e capaz de proporcionar as necessárias garantias, (2) a avaliação da real necessidade e pertinência do uso de dados pessoais e, muito importante, (3) a proporcionalidade deste uso em relação aos fins almejados; (4) a consideração da efetividade dos direitos dos titulares de dados; (5) a elaboração de mecanismos de segurança proporcionais aos riscos presentes, dentre vários outros. A ausência deste conjunto de garantias, hoje, ameaça calcificar práticas deletérias às liberdades fundamentais, empacotadas dentro de burocráticas rotinas administrativas que são impermeáveis aos reais efeitos dos tratamentos dos dados pessoais aos cidadãos e à sociedade.

A proteção de dados no Brasil é uma disciplina para cuja legitimidade e formação contribuíram diversos atores, desde a propositura do Anteprojeto de Lei sobre Proteção de Dados pelo Poder Executivo, passando pelo protagonismo do Poder Legislativo ao encaminhar a matéria até culminar com o reconhecimento por esta Egrégia Corte do Direito Fundamental à Proteção de Dados - a partir do que o caminho trilhado não teria mais retorno.

Paradigmas, no entanto, costumam ser ultrapassados gradualmente. Cabe, neste momento, ao se decidir sobre a constitucionalidade do Decreto 10.046, proporcionar ao cidadão segurança para que reconheça no Estado um digno depositário de seus dados, em uma relação que, ao cabo, é indispensável para que se possibilite o uso e compartilhamento de dados com legitimidade, segurança e sob os auspícios da boa-fé e no marco da defesa do Estado Democrático de Direito.

A atual estrutura do Decreto 10.046 torna inviável esta superação de paradigma. Sua manutenção consolidaria um sistema dúplice de proteção de dados, um para os tratamentos realizados pelo setor privado e outro, débil e desarticulado, para o setor público, configurando óbice à consolidação do direito fundamental à proteção de dados na ordem jurídica pátria, com o agravante de incidir com maior gravidade em relação aos direitos da parcela da população de menor poder aquisitivo ou em situação de vulnerabilidade, para os quais os serviços públicos são ainda mais importantes ou imprescindíveis. Eventualmente, pode ser pertinente que a cessação dos efeitos do Decreto seja modulada em termos definidos por esta Egrégia Corte, de forma a não interromper tratamentos de dados de maior relevância e menor potencial de risco, até o momento em que vier a advir legislação que contemple o novo paradigma, que se afigura, conforme verificamos, ser indispensável e da máxima urgência.

Por todo o exposto, o Conselho Federal da Ordem dos Advogados do Brasil, em iniciativa que contou com a valorosa e indispensável liderança e empenho, entre tantos, das advogadas e advogados Estela Aranha, Lúcia Teixeira Ferreira, Ilton Robl Filho e Marcus Vinícius Furtado Coelho requer, reconhecida a natureza constitucional do direito à proteção de dados pessoais e as razões de fato e de direito aqui aludidas, a declaração da inconstitucionalidade do Decreto 10.046, de 9 de outubro de 2019 em sua íntegra.

31 de agosto de 2022.